Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE

Day 2 - New Employee Onboarding

NAVSEA WARFARE CENTERS Carderock

Human Resources Division - Staffing Branch

Captain Todd E. Hutchison
Commanding Officer, NSWCCD

Larry Tarasek
Technical Director, NSWCCD

WELCOME BACK!

NAVSEA WARFARE CENTERS Carderock Division

Access your onboarding presentation slides on the Carderock New Hires Page :

https://www.navsea.navy.mil/Home/Warfare-Centers/NSWC-Carderock/Career-Opportunities/Forms-for-New-Hires

Once you have obtained your CAC, use the link below to available more useful onboarding materials on your NMCI computer (CAC required):

https://wiki.navsea.navy.mil/display/WDP/Employee+Onboarding+Program

Onboarding – Day 2

Agenda

<u>Day 2</u>

0845	**Welcome /New Employee Roll Call**
0900	**Antiterrorism Level I and Active Shooter Training**
0930	**Workforce Development Overview**
1010	**Break 1**
1020	**Military Protocol Brief**
1050	**Command Evaluation & Review Brief**
1115	**Lunch**
1200	**Initial Security Orientation and Indoctrination Brief**
1230	**Privacy & Personally Identifiable Information & Controlled Unclassified Information**
1300	**Break 2**
1310	**Uncle Sam’s Operations Security and Physical Security / Insider Threat Training**
1340	**Unauthorized Commitments (UACs)**
1400	**Questions / Wrap-Up**

Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE

DoD Level-1 Antiterrorism (AT) Training for New Hires

Homer Renshaw

1052 (Security Division)

Captain Todd E. Hutchison
Commanding Officer, NSWCCD

Larry Tarasek
Technical Director, NSWCCD

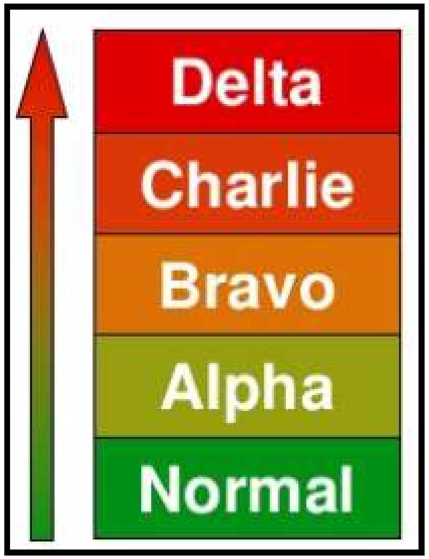
Introduction

- Threat is a real and present danger
- Remain vigilant while executing responsibilities
- International terrorist network may be present where you serve
- Personal safety is important
  - Remain alert
  - Be aware of your surroundings
  - Report suspicious activity
  - Pay attention to antiterrorism briefings
  - Make security part of your routine
- Do not be a tempting target!

America's effort to fight terrorism includes everyone.

Force Protection Conditions

- US military facilities use protective measures organized in a system called Force Protection Conditions, or FPCONs.
- FPCONs are organized in five levels with increased protection at each level:
  - NORMAL
  - ALPHA
  - BRAVO
  - CHARLIE
  - DELTA.



Delta
Charlie
Bravo
Alpha
Normal

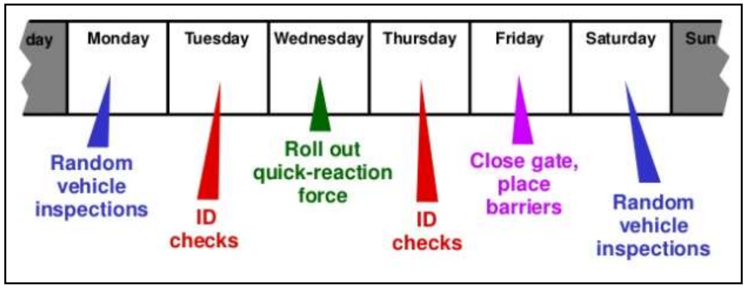
As the threat of attack changes, Commanders change the FPCON to protect personnel

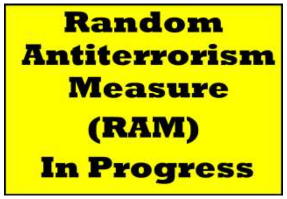
FPCONs (cont.)

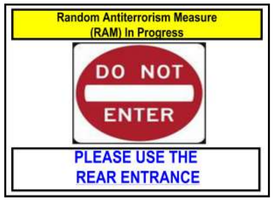
- NORMAL – Routine security posture (access controls)
- ALPHA – Increased threat (maintain indefinitely)
- BRAVO – Increased/predictable threat (operational effects)
- CHARLIE – Per intel, event likely (prolonged hardships)
- DELTA – Actual/imminent event (not for extended duration)

Random Antiterrorism Measures (RAM)

- Supplement FPCONs
- Countermeasure to hostile force observation
- HHQ approval
- Provides change to security atmosphere

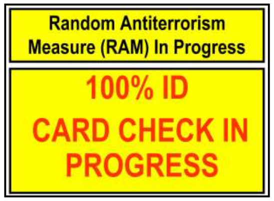

day
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sun
Random vehicle inspections
ID checks
Roll out quick-reaction force
ID checks
Close gate, place barriers
Random vehicle inspections


Random Antiterrorism Measure (RAM) In Progress

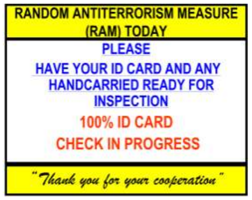

Random Antiterrorism Measure (RAM) In Progress

DO NOT ENTER

PLEASE USE THE REAR ENTRANCE


Random Antiterrorism Measure (RAM) In Progress

100% ID CARD CHECK IN PROGRESS


RANDOM ANTITERRORISM MEASURE (RAM) TODAY

PLEASE HAVE YOUR ID CARD AND ANY HANDCARRIED READY FOR INSPECTION

100% ID CARD CHECK IN PROGRESS

"Thank you for your cooperation"

Anticipate

- Anticipating threats, risks, and vulnerabilities is fundamental to antiterrorism and personal security.
- Ways to do this include:
  - Research criminal activity
  - Understand the tactics & techniques
  - Know types of targets and locations
- Consider consulting these sources
  - Police crime reports
  - Other internet and media resources

Several sources allow you to research threats for yourself

Be Vigilant

- Vigilance is required to continuously observe your surroundings and recognize suspicious activities.
- Understand your environment's normal conditions.
- Knowledge of the normal amplifies abnormal activities.
  - Items that are out of place
  - Attempted surveillance
  - Circumstances that correspond to prior criminal activity in your area

Informed vigilance is fundamental to personal security

Don't Be a Target

- Blend in with your surroundings.
  - Do not wear clothing or carry items that attract criminal attention
  - Remain low key
  - Avoid high criminal locations
- Reduce your vulnerability and exposure:
  - Select places with security measures
  - Be unpredictable
  - Travel in a small group
  - Use automobiles and residences with adequate security features

DOD affiliation may identify you as a potential target

Report and Respond

- Report suspicious activities to appropriate authorities.
  - Report suspicious activity, do not try to deal with it yourself
  - In threatening situations, take steps to reduce your exposure
  - Follow the instructions of emergency pers and first responders

(The Fort Dix attack plot was thwarted by an alert store clerk)

Security is a team effort

Active Shooter Intro

NAVSEA WARFARE CENTERS Carderock Division

- An Active Shooter incident can occur any time, any place
  - September 2013 shooting at the Navy Yard
  - March 2011 shooting of Air Force personnel at Frankfurt Airport in Germany
  - November 2009 shooting at the Soldier Readiness Center in Fort Hood, Texas
  - June 2009 shooting at the Holocaust Museum in Washington, D.C.
  - May 2009 shooting of soldiers outside a military recruitment center in Arkansas
  - 2007 plot to attack Fort Dix using automatic weapons

- Active Shooter incidents are unlikely, but you should be prepared for the possibility.

An incident can occur anywhere, even on your own installation

Active Shooter Fundamentals

NAVSEA WARFARE CENTERS Carderock Division

- Responses to an Active Shooter include:
  - Run
    - If you can escape the area, do so without hesitation
  - Hide
    - If unable to escape, find a place to hide
  - Fight
    - As a last resort, and only if your life is in immediate danger, alone, or as a group, attempt to incapacitate the shooter.

Run, Hide, Fight

Responding to an Active Shooter

- Evacuate: If possible, be sure to:
  - If you can escape, do so without hesitation. Be aware that your evacuation point may be different than for fire evacuations.
  - Evacuate whether others agree to or not.
  - Leave your belongings behind.
  - Help others escape, if possible. Assist individuals with special needs or disabilities.
  - Attempt to rescue others or treat the injured only if you can do so without further endangering yourself or others.
  - Keep your hands visible as you flee.
  - Prevent others from entering the area, if possible.

Run

Responding to an Active Shooter 2

- If unable to escape, find a place to hide.
- Your hiding place should:
  - Be out of the shooter’s view.
  - Provide protection from shots fired (e.g., hide behind large items that afford protection).
  - Prevent shooter from entering (e.g., barricade the door with furniture).
- Silence cell phones/turn off any source of noise (e.g., radios).
- Remain quiet.
- Identify improvised weapons.
- Attempt to rescue others or treat injured only if you can do so without further endangering persons inside a secured area

Hide

Responding to an Active Shooter 3

NAVSEA
WARFARE CENTERS
Carderock Division

- As a last resort, and only if your life is at immediate risk, together or alone, attempt to incapacitate the shooter.
  - Act as aggressively as possible against the shooter.
  - Throw items and improvised weapons.
  - Yell.

- Be committed to your actions until the threat is eliminated.

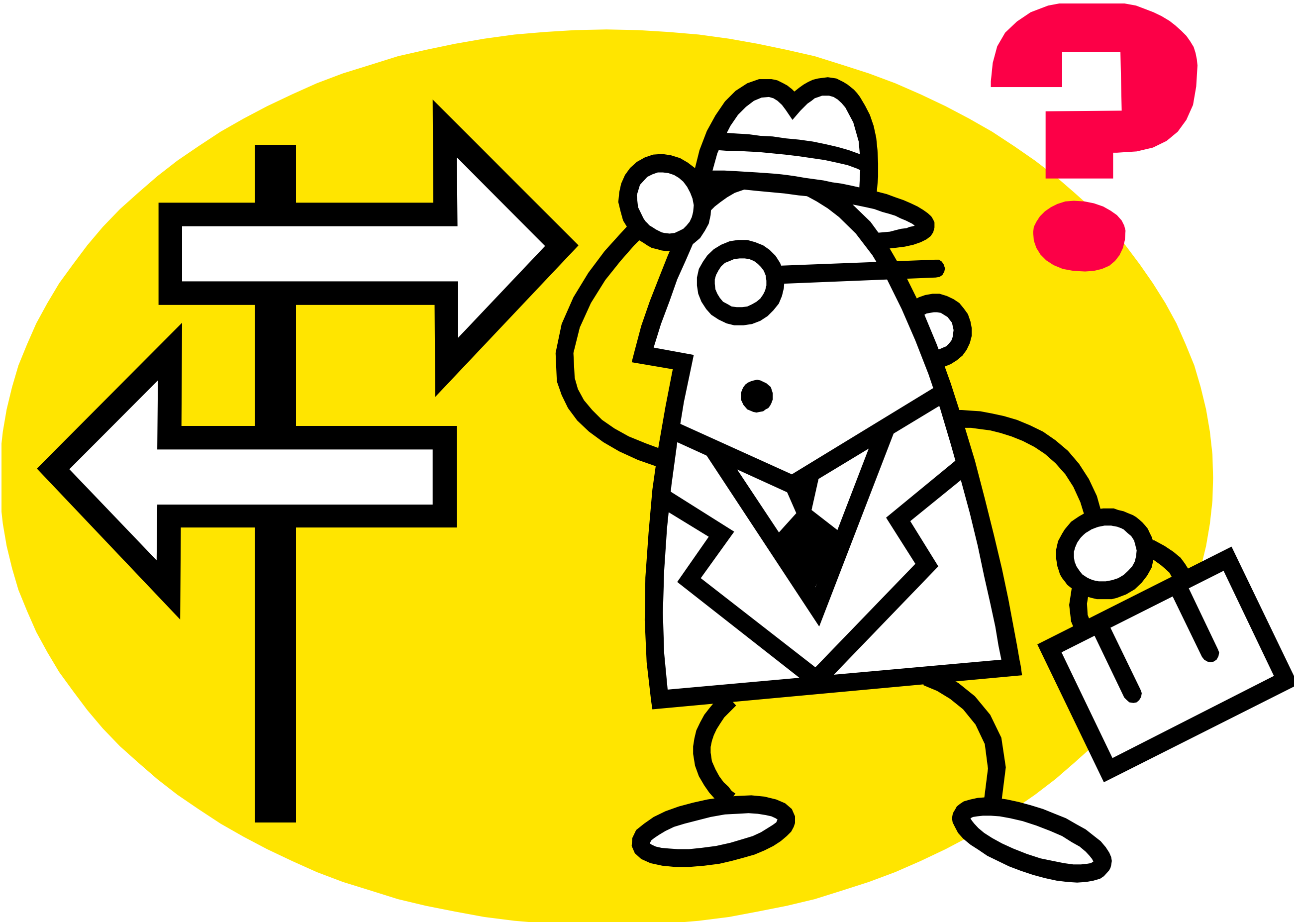
Fight

Arrival of First Responders

- When first responders arrive, support their efforts and do not be a distraction:
  - Officers will move directly to where last shots were heard.
  - Remain as calm as possible and follow Officer's instructions. You may be searched.
  - Avoid quick movements, do not point.
  - Put down items in your hands; raise hands and keep hands visible at all times.
  - Officers may shout commands and push individuals to the ground for their safety.
  - Do not attempt to hold onto Officers for safety.
  - Do not stop to ask Officers for help - proceed in the direction they have approached from.
  - Remember, LE's mission upon arrival is to stop the shooter, rendering aid is secondary.

Cooperate with first responders and don't be a distraction

Questions



NSWC Carderock
NAVSEA
PERSONNEL
INFOSEC
COMSEC
OPSEC
AT/FP
SETA
PHYSICAL
INDUSTRIAL
NSWCCD
Code
105
Security Division

Naval Surface Warfare Center, Carderock Division
AMERICA'S FLEET STARTS HERE

Olamidayo Diana Odusanya, WFD, Code 1016

WFD 2-Day Onboarding Brief (Code 1016)

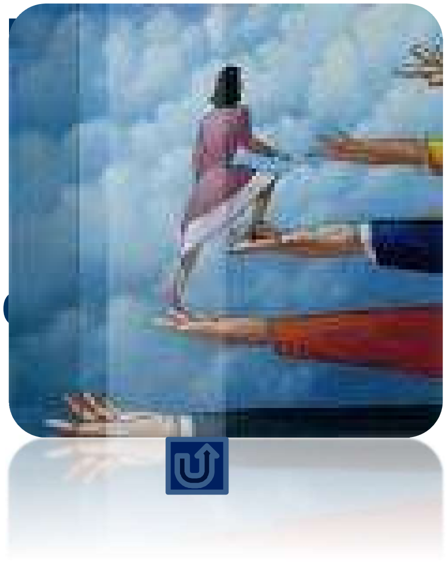
Distribution Statement A: Approved for Public Release; unlimited distribution.

- Mission/goal
- WFD Point of Contacts
- Training Topics
- Training Request (ATR & SF182)
- TWMS
- IDP
- Mandatory Training
- Supervisor Training
- Leadership program (With PROPEL)
- Onsite Training
- Mentoring
- DAWIA
- Extended Term Training
- Scientist & Engineer Development Program (SEDP)
- Learn more at Onboarding Follow-Up

Provide high quality, timely and relevant employee development programs that enhance individual knowledge, skills and abilities.

Develop employees that have the skills that al
division to meet our customers needs.

Provide programs that develop a well-rounde



Olamidayo Diana Odusanya
olamidayo.d.odusanya.civ@us.navy.mil
(240) 274-9362
Training Purchase Card Holder - Code 80
Program Manager for Leadership Development Programs (LEAD, LDP, ALDP), Carderock 101

Linda Florian
linda.k.florian.civ@us.navy.mil
(301) 204-4146
Approving Official for WFD Purchase Card Holders
Program Manager for DAWIA, Onsite Training, Scientist Engineer Development Program (SEDP), Extended Training ETT Program

Jorge Galindo
jorge.l.galindomelecio.civ@us.navy.mil
(301) 742-9701
Training Officer - Workforce Development Branch Head

Renard Walker
renard.c.walker.civ@us.navy.mil
(301) 318-4285
Training Purchase Card Holder - Code 70, Code 02
Program Manager for Mandatory Training, Linked-In

Cecelia Paulding
cecelia.g.paulding.civ@us.navy.mil
(240) 274-9702
Training Purchase Card Holder - Code 60
Program Manager for Individual Development Plan (IDP), Defense Acquisition Workforce Improvement Act (DAWIA)

Jeffrey Klimczak
jeffrey.a.klimczak.civ@us.navy.mil
(301) 275-2517
Training Purchase Card Holder - Code 00, Code 01, Code 03, Code 10, NSWC/NUWC HQ
Program Manager for Supervisor Training, PROPEL, Carderock University, NPS

Open to all employees in Wide range of to

- Technical/Professional Development
- Employee Development
- Leadership, Supervisory

How to access & learn about potential training

- All Hands Emails
- TWMS
- Carderock Intranet
- Course Catalog
- Internet

AdHoc Training Requests (ATR) and SF182

Please remember that an employee shall only attend a class or training if the following events have been executed PRIOR to the employee starting the class or training:

Employee must receive a final confirmation by way of Workflow response (example: Ad-Hoc Training Request (ATR) has been approved by ALL ATR Approving Officials. Purchase Order 4550XXXXXXX has been created. The SF-182 Form can be printed at your convenience.) The purchase card holder then routes the SF-182 to Linda Florian for final review and signature. Once Linda's signature has been obtained on the SF182, payment for the training request (SF-182/ATR) can be rendered.

Employee must receive an email from the purchase card holder indicating that the course has been paid for.

Training requests received after the employee is enrolled and/or begins training without the appropriate approvals is an **Unauthorized Commitment** (UAC). In this situation, the training request will be sent to Code 02 for UAC processing. Employees who enroll in training without prior approval will be held responsible for the total cost of the training.

Approved Individual Development Plan in TWMS

Submit support documents (invoice, quote, account info., etc.)

Must be entered into Navy ERP NLT three weeks prior to class start date

- Enter as soon as possible
- Let us know of any special requirements or payme

Submit ATR in Navy Enterprise Resource Program (ERP)

- Employee, Admin Officer or Training Coordinator enters
- Must be approved by Supervisor

Do <u>NOT</u> attend training until fully approved

- Workforce Development is final approval
- Attending course with approval constitute an Un-authorized Commitment (UAC) violation

No-Show – Department still pays (employee may be require to payback training cost)

Provide proof of training completion

Purchase Card holders for Training/Conferences:

Olamidayo Odusanya

Renard Walker

Cecelia Paulding

Jeffrey Klimczak

Helpful Documents / Resources

Form SF182

Continued Service Agreement

Cost-Comparison Sheet

Graduate Course Guide (If you submit training request for your university or college course)

See CARDEROCKDIVINST 12410.13C or SECNAVINST 12410.25A for reference regulations

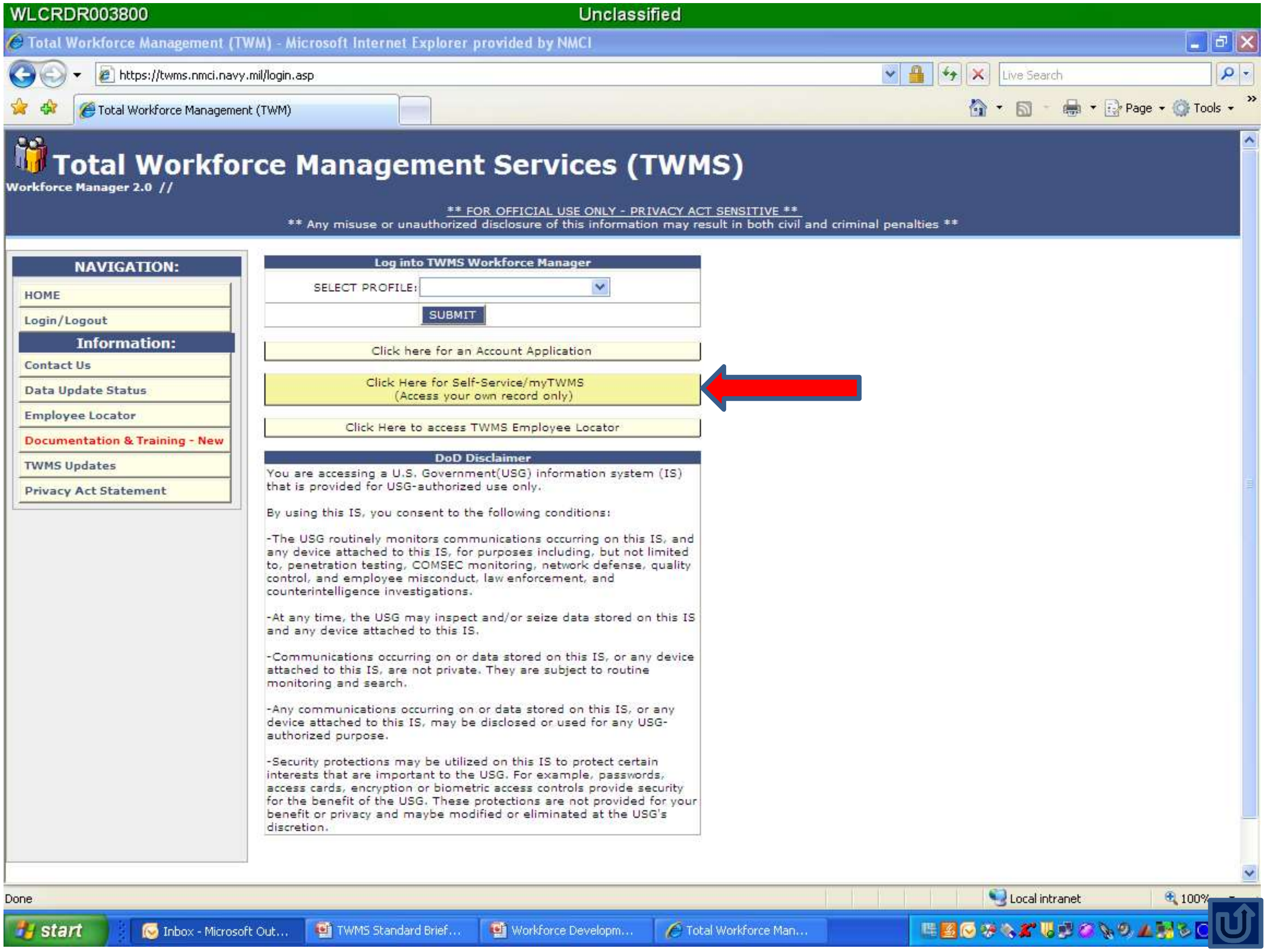
For more information check out

Ad Hoc Training Request Process - Workforce Development Page - NAVSEA Wiki (navy.mil)

Total Workforce Management Service (TWMS) is a government application which gathers information from a number of official programs of record and combines all this data to allow the user to manage their workforce via one easy-to-use web interface. TWMS provides employees access to a number of training courses and allows them to view their personal information such as Notifications of Personnel Action (SF50s).

To access TMWS, employee must have a Common Access Card (CAC) Access

Total Workforce Management Services (TWMS) Quick User Guide



Total Workforce Management Services (TWMS)

Workforce Manager 2.0 //

** FOR OFFICIAL USE ONLY - PRIVACY ACT SENSITIVE **

** Any misuse or unauthorized disclosure of this information may result in both civil and criminal penalties **

Log into TWMS Workforce Manager

SELECT PROFILE:

Click here for an Account Application

Click Here for Self-Service/myTWMS
(Access your own record only)

Click Here to access TWMS Employee Locator

DoD Disclaimer

You are accessing a U.S. Government(USG) information system (IS) that is provided for USG-authorized use only.

By using this IS, you consent to the following conditions:

-The USG routinely monitors communications occurring on this IS, and any device attached to this IS, for purposes including, but not limited to, penetration testing, COMSEC monitoring, network defense, quality control, and employee misconduct, law enforcement, and counterintelligence investigations.

-At any time, the USG may inspect and/or seize data stored on this IS and any device attached to this IS.

-Communications occurring on or data stored on this IS, or any device attached to this IS, are not private. They are subject to routine monitoring and search.

-Any communications occurring on or data stored on this IS, or any device attached to this IS, may be disclosed or used for any USG-authorized purpose.

-Security protections may be utilized on this IS to protect certain interests that are important to the USG. For example, passwords, access cards, encryption or biometric access controls provide security for the benefit of the USG. These protections are not provided for your benefit or privacy and maybe modified or eliminated at the USG's discretion.

Individual Development Plan (IDP) are mandatory for all employees in order to provide an opportunity for supervisor and employees to identify training that will ensure employee professional and organizational performance. The IDP is a developmental tool to help employees attain and improve their knowledge, skills, and abilities necessary for enhanced job performance and to help them achieve personal and career goals.

Access to employee's Individual Development Plan (IDP) is located in TWMS: https://twms.dc3n.navy.mil/

Resources:

CARDEROCK DIV NOTICE 12410 - Mandatory IDP Implementation

COMPLETING THE TWMS IDP GUIDE

To learn more, go to **IDP - Workforce Development Page - NAVSEA Wiki (navy.mil)**

Training mandated by executive order, Federal statute, regulation or at the direction of the Secretary of the Navy is referred to has mandatory training and is required to be completed by all civilian employees on a reoccurring basis. Additional training are required to be completed by supervisors and new Employees.

TWMS is the location to complete all non-safety related mandatory training. Training is announced via All Hands email and once the training is completed, employee's TWMS training record is updated accordingly. TWMS: https://twms.navy.mil/

To learn more, go to about this program:

PRIOR TO ONBOARDING:

- Cyber Awareness – DOD-IAA-V19.0

DAY 1:

- Initial Security Brief – CMD-SECBRIEF INITIAL
- Cybersecurity 101 – TWMS-610848
- Initial Information Assurance Brief
- EEO Training Brief – TWMS-614600
- Constitution Day – TWMS-689046 (part of CO brief)
- Time & Attendance – TWMS-690336
- Ethics – TWMS-689045 (for new employee only)
- Records Management – DOR-RM-010-1.2
- Telework – TWMS-OCHR-EMP1 (for new employee only, not the one for supervisor)

DAY 2:

- PII – DON-PRIV-2.0
- CUI – TWMS-686564
- OPSEC – NOST-USOPSEC-4.0
- Active Shooter – TWMS-687121
- Anti-terrorism Level 1 – CENSECFOR-AT-010-2.0
- Physical Security – TWMS-681607
- Workplace Violence – TWMS-658532
- Derivative Classifiers – TWMS-571920

ONBOARDING FOLLOW-UP:

- POSH – TWMS-613963
- NO FEAR – TWMS-613957
- Counterintelligence Awareness (NCIS) – DON-CIAR-1.0
- SAPR Initial (One Team, One Flight) – TWMS-577914 /TWMS-693475

As a supervisor there are several training requirement and we have developed a toolkit to assistance with that.

For more information about Supervisor Mandatory Training requirements, please visit our Supervisor Toolkit wiki page below: https://wiki.navsea.navy.mil/display/WDP/Supervisor+Toolkit

PROPEL Launch for Supervisors

- Propel Launch is a 5-day course for **new first-line supervisors** at the Warfare Center Divisions, NAVSEA HQ, PEOs and Field Activities.
- Must be completed within **first year** of supervisory assignment.
- Propel Launch provides an introductory level awareness of the NAVSEA expectations for supervisors and the interactive class content aids a new supervisor in interpreting the workplace environment to identify and utilize organizational resources in order to take appropriate and timely supervisory

PROPEL Launch for Supervisors

NAVSEA
WARFARE CENTERS
Carderock Division

- Courses are held monthly at 1 of the 10 Warfare Centers or NAVSEA HQ, either in person or virtually.
- The student's home Division covers the labor and any travel costs required for the student to attend Propel. How the Division chooses to allocate these costs is at their discretion.
- There is no tuition or registration cost associated with the Propel training.

Propel FY22 Course Dates and locations:

Course Dates	Location	Onsite or Virtual
07-11 Feb	NUWC Newport	FULL (Completed)
28 Feb - 04 Mar	NSWC Panama City	FULL
28 Mar - 01 Apr	Keyport, WA	In-Person
25-29 Apr	Corona, CA	In-Person

Carderock is dedicated to building new leaders and transforming leaders to better service our missions. To keep in line with this goal, varies Leadership Development Program opportunities are available for employees to enhance their leadership skills and abilities. These programs are grade specific and vary in program duration.

To learn more about these programs or for latest updates, go to:

Carderock Advanced Leadership Development Programs - Workforce Development Page - NAVSEA Wiki (navy.mil)

Current leadership programs offered:

Bridging the Gap Leadership Development Program

Executive Leadership Development Program (ELDP)

White House Leadership Development Program (WHLDP)

Dwight D. Eisenhower School for National Security and Resource Strategy Senior for Non Acquisition Course (ES)

Capitol Hill Fellowship Program (CHFP) (AKA, Navy Legislative Fellowship Program (NLFP)

Commander's Executive Fellows Program (CEFP)

Federal Internal Coach Training Program (FICTP)

Federal Executive Institute (FEI) - Leadership for a Democratic Society (LDS)

Defense Civilian Emerging Leader Program (DCELP)

President's Management Council (PMC) Interagency Rotation Program (IRP) or (PMC-IRP)

Defense Senior Leader Development Program (DSLDP)

Journey Level Leader Program (JLL)

Next Generation Leadership Program (NextGen)

The Workforce Development Branch offers a variety of on-site training courses that have been created to develop and maintain a capable, diverse, and highly-motivated workforce.

Courses are held from 0800 to 1530; half-day classes are conducted from 0800 to 1200 unless otherwise specified.

To learn more, contact Workforce Development Branch or go to On-site/Virtual Command-Wide Training - Workforce Development Page - NAVSEA Wiki (navy.mil)

Employees are encouraged to develop mentoring relationships throughout their career at NSWCCD. Through these partnerships, employees develop their knowledge, skills, abilities, and/or thought process through an exchange of different perspectives. The NSWCCD HR Division provides employees with resources and assistance for cultivating mentoring relationships that grow and change according to your professional objectives.

Resources:
DOD Mentoring Resource Portal
Linked-In Learning
NAVSEA HQ Mentor Program

To learn more, go to Mentoring Program - Workforce Development Page - NAVSEA Wiki (navy.mil)

The Defense Acquisition Workforce Improvement Act (DAWIA) was enacted to improve the effectiveness of the military and civilian acquisition workforce through enhanced education, training and career development thereby improving the acquisition process. If you occupy a designated acquisition position, DOD's certification standards apply to you.

Resources:

2017 DON DAWIA Operating Guide

DAWIA Core Plus Certification Standards

For more information, go to Carderock DAWIA **intranet page** **or** **DAWIA - Workforce Development Page - NAVSEA Wiki (navy.mil)**

The Extended Term Training (ETT) Program provides funds for employees who are pursuing a graduate or doctoral degree in an area that supports one of the Division's core equities. The program allows selected employees to attend classes on a full, three-quarter, or half-time basis. Employees can apply for salary, tuition and academic fees to complete their graduate or doctoral degree.

The ETT Program allows for off-site training away from the job for more than 120 consecutive days as defined below:

Full Time: 40 hours per week

Three Quarter Time: 30 hours per week

Half Time: 20 hours per week

The SEDP includes all entry-level professional scientists and engineers located at all NSWCCD sites. Entry level may be at either the ND-II or ND-III levels. The SEDP is a two or three year professional development program consisting of SEDP meetings, on-the-job experiences, required courses, special developmental courses, established mentor/mentee relationships, and a minimum of two career development assignments. Successful completion of these program elements will qualify the participant for advancement to the full performance level of ND-IV scientific or engineering position.

Code 1016 will maintain training records and files; evaluate program compliancy against regulations, directives, and instructions.

The purpose of this training is to inform interested employees about Carderock's mission and to give them a better understanding of how each Carderock department supports that mission.

Carderock 101 *(183 MB - PowerPoint presentation with video)*
Carderock 101 *(4.4 MB - PDF version of slides only)*

Note: SEDP employees are required to complete this training.

To learn more, contact Workforce Development Branch

During Onboarding Follow-up Session, WFD program managers will be available to chat and share updates to new employee about:

- Individual Development Plan (IDP)
- Mentoring Opportunities
- Defense Acquisition Workforce Improvement Act (DAWIA)
- Scientist Engineer Development Program (SEDP)
- Extended Term Training (ETT) Program

Questions?

Break 1

Break - 1

NAVY AND MILITARY PROTOCOL

Last Updated 12 October 2021

AMERICA'S FLEET STARTS HERE

Topics to be Covered

- Department of Navy (DoN) Civilians
- Military Personnel
- Addressing Military Personnel
- Navy Terminology
- Some Basic Navy Customs
- Riding a Ship

Life as a DoN Civilian

Working as a DoN civilian places you in a different culture from a standard position in private industry.

Generally, you will work with and for civilians, but there are some differences between our work environment and private industry you should know...

- Our command chief executive is a Navy Captain
- You will likely have many opportunities to work directly with Navy, Marine, and other military officers and enlisted personnel
- Many of our processes are based on military instructions, regulations or practices
- Military names and acronyms pervade our work vocabulary
- When working on ships, there is an expectation that civilians know some basic things about ship life, terms and customs
- The military traditions and ceremonies are very powerful and motivating - civilians are expected to be familiar with them

Three Categories of Military Personnel

- **Officers** – Are commissioned by the President and are highly educated, specially trained military leaders who manage the Navy's personnel, ships, aircraft, and weapons systems.

- **Warrant Officers** – Specialists in their fields who are selected for positions between the ranks of officer and enlisted personnel (US Air Force does not have these)

- **Enlisted** – Those who enlist in the service as non-officers and who perform the numerous specialized tasks that accomplish the mission

Officers

Officers are generalists trained to make decisions and lead organizations of various levels of responsibility and complexity.

In the Navy

- O-1 through O-4 are junior grade officers
- O-5 and O-6 are senior officers
- O-7 through O-10 are flag officers

In the Marine Corp

- O-1 through O-3 are company grade officers
- O-4 through O-6 are field grade officers
- O-7 through O-10 are general officers

In the civilian leadership structure of the United States military, the Marine Corps is a component of the United States Department of the Navy (DoN).
In the military leadership structure, the Marine Corps is a separate branch.

Navy and Marine Corps Officer Titles

In the Navy

- O-1 Ensign (ENS)
- O-2 Lieutenant Junior Grade (LTJG)
- O-3 Lieutenant (LT)
- O-4 Lieutenant Commander (LCDR)
- O-5 Commander (CDR)
- O-6 Captain (CAPT)
- O-7 Rear Admiral Lower Half (RDML) – 1 star
- O-8 Rear Admiral Upper Half (RADM) – 2 star
- O-9 Vice Admiral (VADM) – 3 star
- O-10 Admiral (ADM) – 4 star
- None – Fleet Admiral (Wartime Only)

In the Marine Corps

- O-1 2ND Lieutenant (2nd Lt.)
- O-2 First Lieutenant (1st Lt.)
- O-3 Captain (Capt.)
- O-4 Major (Maj.)
- O-5 Lieutenant Colonel (Lt. Col.)
- O-6 Colonel (Col.)
- O-7 Brigadier General ((Brig. Gen.)
- O-8 Major General (Maj. Gen.)
- O-9 Lieutenant General (Lt. Gen.)
- O-10 General (Gen.)

For a complete chart comparing officer ranks of all service branches, visit the
US DoD Military Officer Rank Insignia Website

How to Interact with Senior Officers

NAVSEA WARFARE CENTERS Carderock Division

As you may interact with senior officers, generally O-6s and higher, below are some protocols to observe:

- At most military installations, stand for Flag Officers and Commanding Officers (CO) when they enter a room or are announced
- Generally, they are an O-6 or higher (Navy Captain or other Service Branch Colonel)
- Sometimes they are announced before entering the room: “Officer on Deck!”
- A salute is not necessary; civilians do not salute
- Officers and CO’s avoid fraternization with enlisted sailors and soldiers – civilians may generally follow suit when in the presence of officers
- Use sir or ma’am when appropriate
- Use proper military speak when discussing common terms such as dates, time or ship terminology
- Adhere to strict standards of timeliness and appearance when you are expecting to meet with a senior officer

Navy Enlisted Titles

In the Navy

- E1 – Seaman Recruit
- E2 – Seaman Apprentice
- E3 – Seaman
- E4 – Petty Officer 3rd Class
- E5 – Petty Officer 2nd Class
- E6 – Petty Officer 1st Class
- E7 – Chief Petty Officer
- E8 – Senior Chief Petty Officer
- E9 – Master Chief Petty Officer or
- E9 – Fleet or Command Master Chief Petty Officer
- E9 – Master Chief Petty Officer of the Navy

Can be addressed as Petty Officer or by their rate. E.g., OS1 for an Operational Specialist First Class Petty Officer.

Can be addressed as Chief, Senior Chief or Master Chief or by their rate. E.g., ETCS for an Electronics Technician Senior Chief.

Rate – The pay grade a person works in

Rating – The specialized field the person trains in or works in

Enlisted Navy personnel do not have a rank, only naval officers do

For a complete chart comparing enlisted rates and ranks of all service branches, visit the US DoD Military Enlisted Rank Insignia Website

USMC Enlisted Titles

WARFARE CENTERS
Carderock Division

In the Marine Corps

- E1 – Private
- E2 – Private First Class
- E3 – Lance Corporal
- E4 – Corporal
- E5 – Sergeant
- E6 – Staff Sergeant
- E7 – Gunnery Sergeant
- E8 – Master Sergeant or First Sergeant
- E9 – Sergeant Major
- E9 – Master Gunnery Sergeant
- E9 – Sergeant Major of the Marine Corps

Rate – The pay grade a person works in

Military Occupational Specialty (MOS) – The specialized field the person trains in or works in (very similar to Navy Rating)

For a complete chart comparing enlisted rates and ranks of all service branches, visit the US DoD Military Enlisted Rank Insignia Website

Non-Commissioned Officers

Navy Petty Officers and USMC Corporals and Sergeants are considered non-commissioned officers (NCOs) (E4 and higher)

Junior NCOs (E4s) function as first tier supervisors and technical leaders

NCOs serving in the top three enlisted grades (E-7, E-8, and E-9) are termed senior NCOs

- Chief Petty Officers in the Navy (and Coast Guard)
- Expected to exercise leadership at a more general level
- Lead larger groups of service members
- Mentor junior officers, and advise senior officers on matters pertaining to their areas of responsibility
- Marine Corps senior NCOs are referred to as Staff NCOs
- A select few senior NCOs serve at the highest levels of their service, advising their service Secretary and Chief of Staff on all matters pertaining to the well-being and utilization of the enlisted force

Navy Terminology

You may hear or be exposed to various Naval terms, particularly if you work with actual ships or people from shipyards. Here are some terms you will want to be familiar with. Many were derived from hundreds of years of naval operations across the globe.

Hull – The outside part of the ship that rides in or above the water line but below the main deck

Bow or Fore – Forward most part of the hull

Aft or Fantail – Back most part of the hull

Keel – The foundation of the ship, it is the very bottom most part of the hull and it usually forms a V or U shape

Stem – The forward most end of the keel

Stern – The after most end of the keel to which the rudder is usually attached

Bulkheads – The walls in the interior of the ship that divide it into compartments

Decks – Floors of the ship

Portholes – Windows of the ship

USS Constitution – "Old Ironsides"

Navy Terminology

You may hear or be exposed to various Naval terms, particularly if you work with actual ships or people from shipyards. Here are some terms you will want to be familiar with. Many were derived from hundreds of years of naval operations across the globe.

Gangway – Walkway between the shore and the ship used for crew and passengers to board or leave

Go Aloft – Climb up ladders to go to higher decks in the ship

Go Below – Climb down ladders to get to lower decks**.**

Passageway – Essentially a walkway or hallway leading to other compartments.

Quarterdeck – Not actually a deck, but a designated compartment where official business and operations of the ship are carried out.

Starboard Side – Right hand side of the ship (looking towards the bow)

Port Side – Left hand side of the ship

USS Constitution in dry-dock during restoration/maintenance

Navy Terminology

Applying ship terminology to buildings is very common. Dam Neck site employees checked in at the Quarterdeck this morning. These terms are also used frequently at the Pentagon or the Washington Navy Yard (WNY).

Quarterdeck – Receptionist desk and area

Decks – Floors in a building

Head – Bathroom

Passageways or P-ways – Hallways

Bulkheads – Walls

Washington Navy Yard

Riding a Ship

You may be assigned at some time to visit a ship to see the technology or system your are working on firsthand. Always remember the Ship is the Sailor's home, and you are an onboard guest. It is therefore important to observe and respect the Navy's customs and courtesies, and to always conduct yourself in a professional manner.

All NSWCCD employees planning to ride a ship will undergo shipboard training to learn the etiquette, safety, and procedures aboard ship.

Manning the Rails - A form of salute or honor; in this case, celebrating return to port

Phonetic Alphabet

Aboard ships, signals are sent to one another as letters and/or numbers, which have meanings by themselves or in certain combinations. In the Allied Signals Book, “BZ” or “Bravo Zulu” means “Well Done”

Phonetic Alphabet

Alpha
Bravo
Charlie
Delta
Echo
Foxtrot
Golf
Hotel
India
Juliet
Kilo
Lima
Mike
November
Oscar
Papa
Quebec
Romeo
Sierra
Tango
Uniform
Victor
Whiskey
X-Ray
Yankee
Zulu

Change of Command Ceremony

- The formal passing of responsibility, authority, and accountability of command from one officer to another
- Rich in naval tradition and quite formal
- The relieving orders are read and the outgoing Commanding Officer has the opportunity to say goodbye. The new Commanding Officer reads the order of assignment to command and officially "reports for duty"
- Generally happens about every 3 years at NSWC Carderock.

Daily Honoring of the Colors

- Colors are honored every day at 0800 and sunset
- If you observe that this ceremony is about to begin, follow these guidelines:
  - If driving, pull over and wait for the ceremony to conclude
  - If walking, stop, face the direction of the flag or music, and cover your heart with your right hand until the ceremony is concluded

Ceremonial Honoring of the Colors at Events

- A Color Guard will move forward with the Flags to present to all people present
- All present rise and face the Color Guard
- The National Anthem is played
- At this time, all military members salute while the music plays
- All civilians remove their hats and place their right hand over their hearts

The Flag may be referred to as: “The Flag”, “The Colors”, “The Standard” or “The National Ensign”

Recognition by the CO or Executive

Navy employees can receive recognition from the CO or an Executive from NSWCCD or another military activity for a job well-done

- A formal letter of recognition may be sent
- A formal awarding of honor or recognition in the correct venue may take place, e.g.:
  - A department technical award
  - A NSWCCD award at the annual awards ceremony

In Closing…

These are just some of the interesting facets of Navy and Military protocol.

For more information on Navy Protocol, you can research several Navy and commercial websites.

Here are a few suggestions:

*Official Site of the United States Navy –*www.navy.mil

Official website of the Department of Defense – www.defense.gov

Naval History and Heritage Command – www.history.navy.mil

Command Evaluation and Review Office (Code 00N)

Command Review & Investigations Office

Staffing:

- Duc Cang, Acting CR&I Director/Investigator
- Vacant, Auditor
- Vacant, Investigator

NSWCCD Instruction 5000.1D

- Command Review & Investigations Program
- CR&I is meant to provide the Commanding Officer (CO) with an independent, in-house assessment capability designed to assist in improving mission accomplishment, integrity of command and economical use of resources. command or activity operations. The CR&I Office is a staff function that reports directly to the CO.

Command Review & Investigations Office

Programmatic Functions:

1. Hotline Program (Fraud, Waste, Abuse & Mismanagement)

- Serves as the focal point for FWA matters, including overall program coordination.

- Conducts investigations and inquiries of internal/ external hotline allegations.

- If appropriate, refers fraudulent cases to Naval Criminal Investigative Service.

2. Command Directed Investigations (CDIs)

- Conducts Management Inquiries, Preliminary Inquiries, JAGMAN investigations and other Command-level Investigations as directed by the Commanding Officer.

Command Review & Investigations Office

3. Command Evaluations/Reviews (Annual Plan)

- Conducts periodic and special reviews, evaluations, studies and analyses of command or activity operations.

- Provides an independent, in-house capability to detect deficiencies, improprieties or inefficiencies.

- Provides recommendations to correct conditions which adversely impact mission accomplishment, command integrity, or efficient use of resources.

4. Audit Liaison/Follow-up

- Serves as Division liaison, and provides logistical and administrative support for the GAO, NAVAUDSVC, DOD IG, and NAVINSGEN.

- Maintains a central depository of audit reports and audit responses to findings and recommendations.

Command Review & Investigations Office

Matters Appropriate for the Inspector General's Hotline

* Abuse of Title/Position

* Bribes/Kickbacks/Acceptance of Gratuities

* Conflicts of Interests

* Ethics Violations

* False Official Statements/Claims

* Fraud

* Gifts (Improper receipt or giving)

* Waste (Gross)

* Misuse of Official Time, Gov't Property, Position and Public Office

* Political Activities

* Purchase Card Abuse

* Reprisal (Military Whistleblower Protection)

* Safety/Public Health (Substantial/Specific)

* Systemic Problems

* Time and Attendance (Significant Violations)

* Travel Card Abuse/Travel Fraud

* Mismanagement/Organ. Oversight (Significant Cases)

QUESTIONS?

REMEMBER THE HOTLINE NUMBER: (301) 227-4228

Visit our Intranet Site:

https://cuthill.aw3s.navy.mil/intra/ig/

How to File a Complaint:

https://cuthill.aw3s.navy.mil/intra/ig/how_to_file.html

NAVSEA Hotline Number: 1-800-356-8464

NAVSEA Hotline Email: NSSC_NAVSEAIGHotline@navy.mil

Lunch

See you back at noon!

Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE

NSWCCD Initial Security Orientation Briefing

Adam Wallmark, Code 1053 Special Programs

Captain Todd E. Hutchison
Commanding Officer, NSWCCD

Larry Tarasek
Technical Director, NSWCCD

Distribution A – Approved for Public Release, Distribution Unlimited

Security Education & Awareness

‘Activities undertaken to ensure that people have the skills, knowledge, and information to enable quality performance of security functions and responsibilities, understand security program policies and requirements, and maintain continued awareness of security requirements and intelligence threats.’

Security Mission

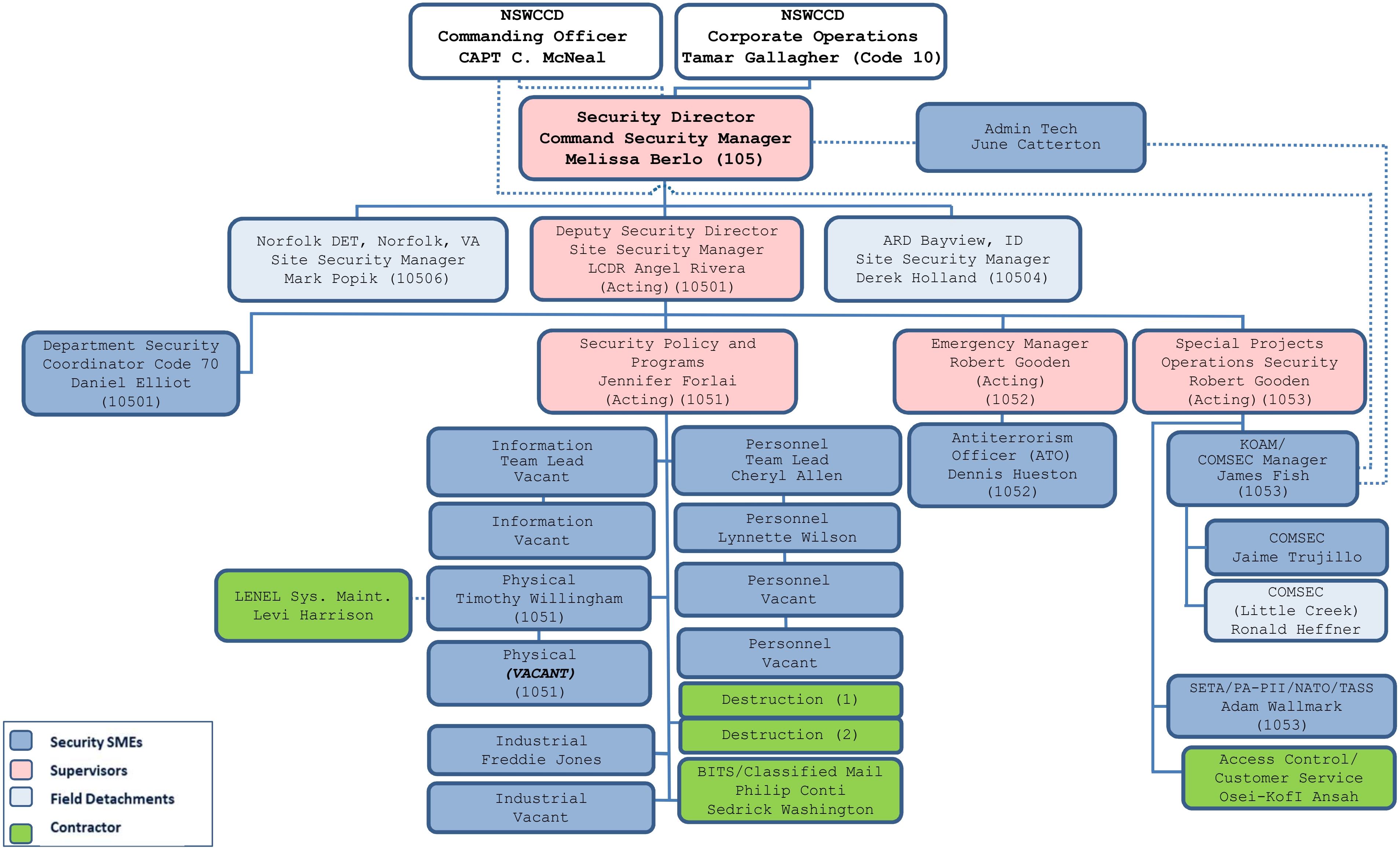
The protection of U.S. Government assets including people, property, and both classified and controlled unclassified information is the responsibility of each and every member of the Department of Navy (DON), regardless of how it was obtained or what form it takes. Our vigilance is imperative. Anyone with access to these resources has an obligation to protect them.

Objectives

- Identify each functional areas and responsibilities of security

- Provide a basic understanding of DOD security policies

Security Division (Code 105)



NSWCCD
Commanding Officer
CAPT C. McNeal

NSWCCD
Corporate Operations
Tamar Gallagher (Code 10)

Security Director
Command Security Manager
Melissa Berlo (105)

Admin Tech
June Catterton

Norfolk DET, Norfolk, VA
Site Security Manager
Mark Popik (10506)

Deputy Security Director
Site Security Manager
LCDR Angel Rivera
(Acting) (10501)

ARD Bayview, ID
Site Security Manager
Derek Holland (10504)

Department Security Coordinator Code 70
Daniel Elliot
(10501)

Security Policy and Programs
Jennifer Forlai
(Acting) (1051)

Emergency Manager
Robert Gooden
(Acting)
(1052)

Special Projects Operations Security
Robert Gooden
(Acting) (1053)

Information
Team Lead
Vacant

Information
Vacant

LENEL Sys. Maint.
Levi Harrison

Physical
Timothy Willingham
(1051)

Physical
(VACANT)
(1051)

Industrial
Freddie Jones

Industrial
Vacant

Personnel
Team Lead
Cheryl Allen

Personnel
Lynnette Wilson

Personnel
Vacant

Personnel
Vacant

Destruction (1)

Destruction (2)

BITS/Classified Mail
Philip Conti
Sedrick Washington

Antiterrorism Officer (ATO)
Dennis Hueston
(1052)

KOAM/
COMSEC Manager
James Fish
(1053)

COMSEC
Jaime Trujillo

COMSEC
(Little Creek)
Ronald Heffner

SETA/PA-PII/NATO/TASS
Adam Wallmark
(1053)

Access Control/
Customer Service
Osei-KofI Ansah

🟦 **Security SMEs**
🟥 **Supervisors**
⬜ **Field Detachments**
🟩 **Contractor**

Code 105 Office Hours

- **Main Hours**
  - 0730-1530
- **Classified Mail Handling/Document Control**
  - 0730 – 1100
  - 1200 – 1500
  - FedEx Drop Offs
    - NLT Noon, prior day
    - Last day/time for pick up Thursday/0900

Personnel Security

Security Clearances

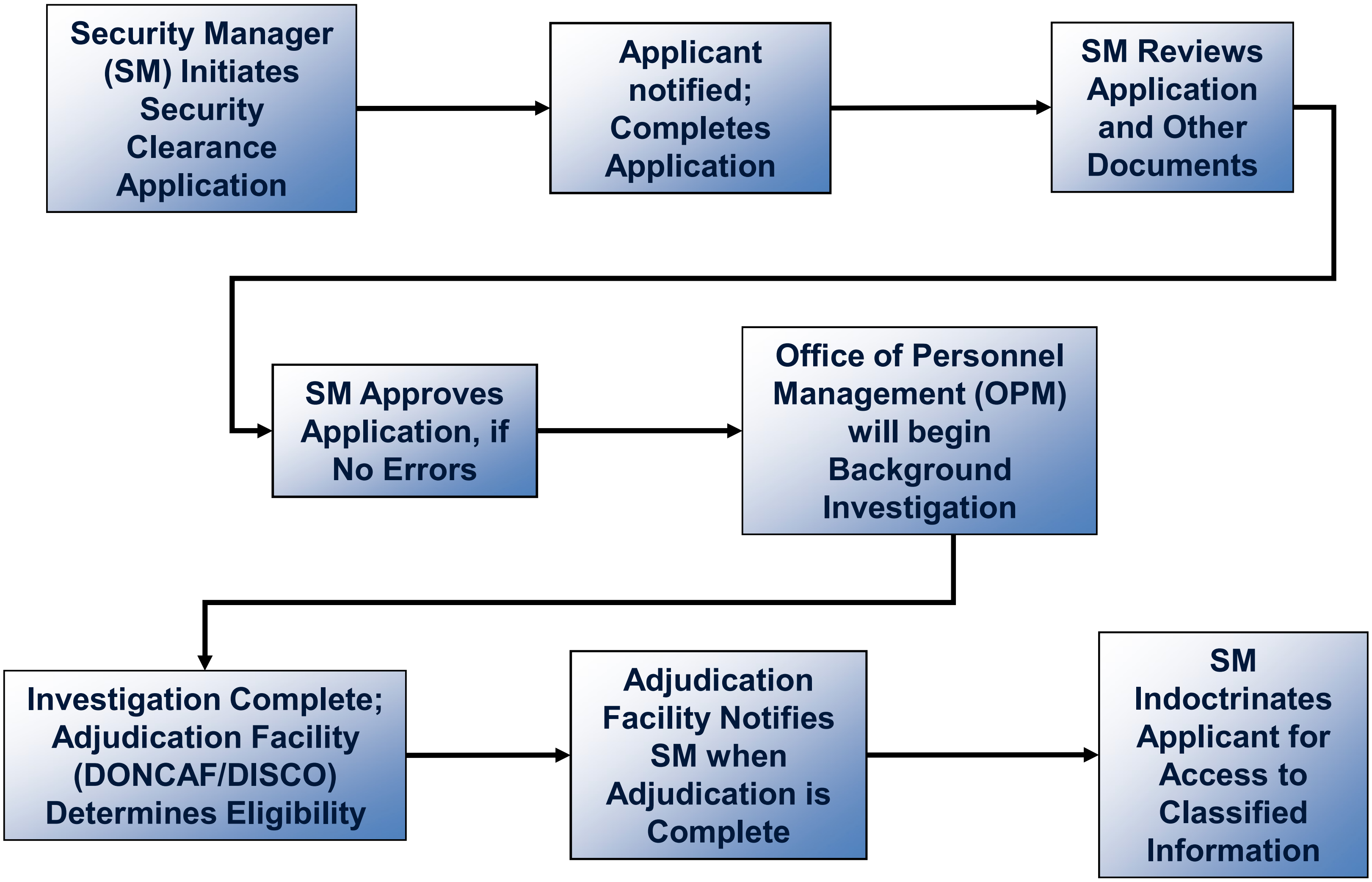
- Employment with the NSWCCD requires you to maintain eligibility for access to classified information
- Completed Electronic Questionnaires for Investigation Processing (e-QIP) system
- Access to classified information will be authorized at the level necessary to perform your duties

Eligibility for Access to Classified Material is a privilege, not a right.

Your Security Clearance

- Position sensitivity and/or duties will determine level of clearance or access
- There are three levels of Security Access Requirements (SAR):
  - Top Secret (TS)
  - Secret (S)
  - Confidential (C)
- You MUST coordinate with your Security Manager for all matters concerning security clearance/access!

Security Clearance Process



Security Manager (SM) Initiates Security Clearance Application

Applicant notified; Completes Application

SM Reviews Application and Other Documents

SM Approves Application, if No Errors

Office of Personnel Management (OPM) will begin Background Investigation

Investigation Complete; Adjudication Facility (DONCAF/DISCO) Determines Eligibility

Adjudication Facility Notifies SM when Adjudication is Complete

SM Indoctrinates Applicant for Access to Classified Information

13 Adjudicative Guidelines

A - Allegiance to the U. S.
B - Foreign Influence
C - Foreign Preference

ALLEGIANCE ISSUES

D - Sexual Behavior
E - Personal Conduct
F - Financial Considerations

CHARACTER ISSUES

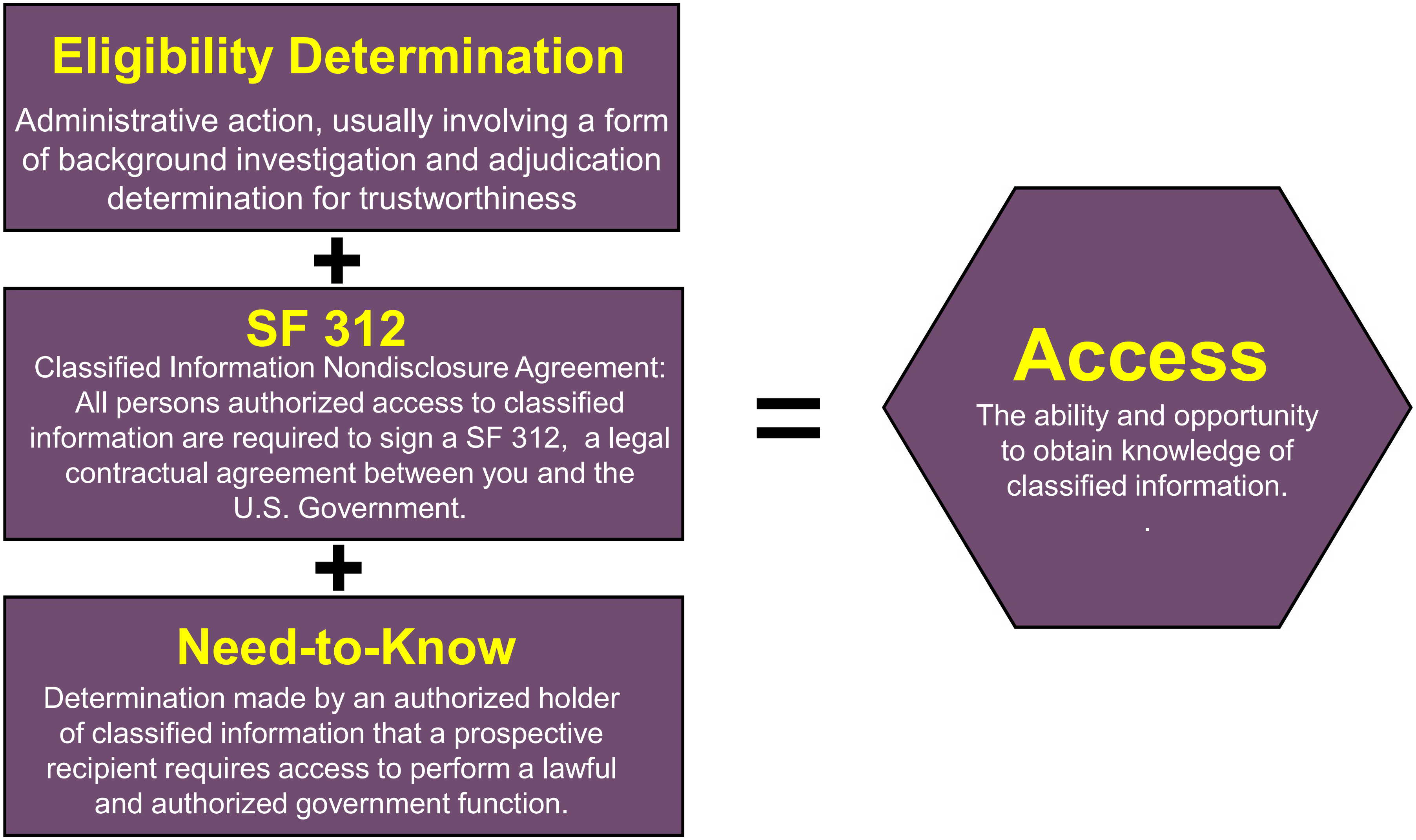
G - Alcohol Consumption
H - Drug Involvement & Substance Abuse
I - Psychological Conditions

HEALTH ISSUES

J - Criminal Conduct
K - Handling Protected Information
L - Outside Activities
M - Use of Information Technology

BEHAVIOR ISSUES

Access Eligibility Process



Eligibility Determination

Administrative action, usually involving a form of background investigation and adjudication determination for trustworthiness

+

SF 312

Classified Information Nondisclosure Agreement: All persons authorized access to classified information are required to sign a SF 312, a legal contractual agreement between you and the U.S. Government.

+

Need-to-Know

Determination made by an authorized holder of classified information that a prospective recipient requires access to perform a lawful and authorized government function.

=

Access

The ability and opportunity to obtain knowledge of classified information.

.

Continuous Evaluation Program

Employees must recognize and avoid behaviors that might jeopardize their security clearance.

In accordance with NSWCCD Policy Statement for Continuous Evaluation Program, dated 22 FEB 17: individuals are required to report to their supervisor or appropriate security personnel and seek assistance for any incident or situation that could affect their continued eligibility for access to classified information. Individuals shall be initially and periodically briefed thereafter, to ensure familiarity with pertinent security regulations and the standards of conduct required of individuals holding positions of trust.

*****The ultimate responsibility for maintaining eligibility to access classified information rests on YOU!*****

Self-Reporting

Self-reporting is mandatory and emphasizes personal integrity

With this privilege comes the obligation to report certain activities

Foreign Travel

Foreign Contacts

Marriage/Divorce

Alcohol Abuse

Drug Use

Bankruptcy/
Credit Issues

Incarceration/
Arrest

Foreign
Allegiance

Loss/Compromise
of Classified Info

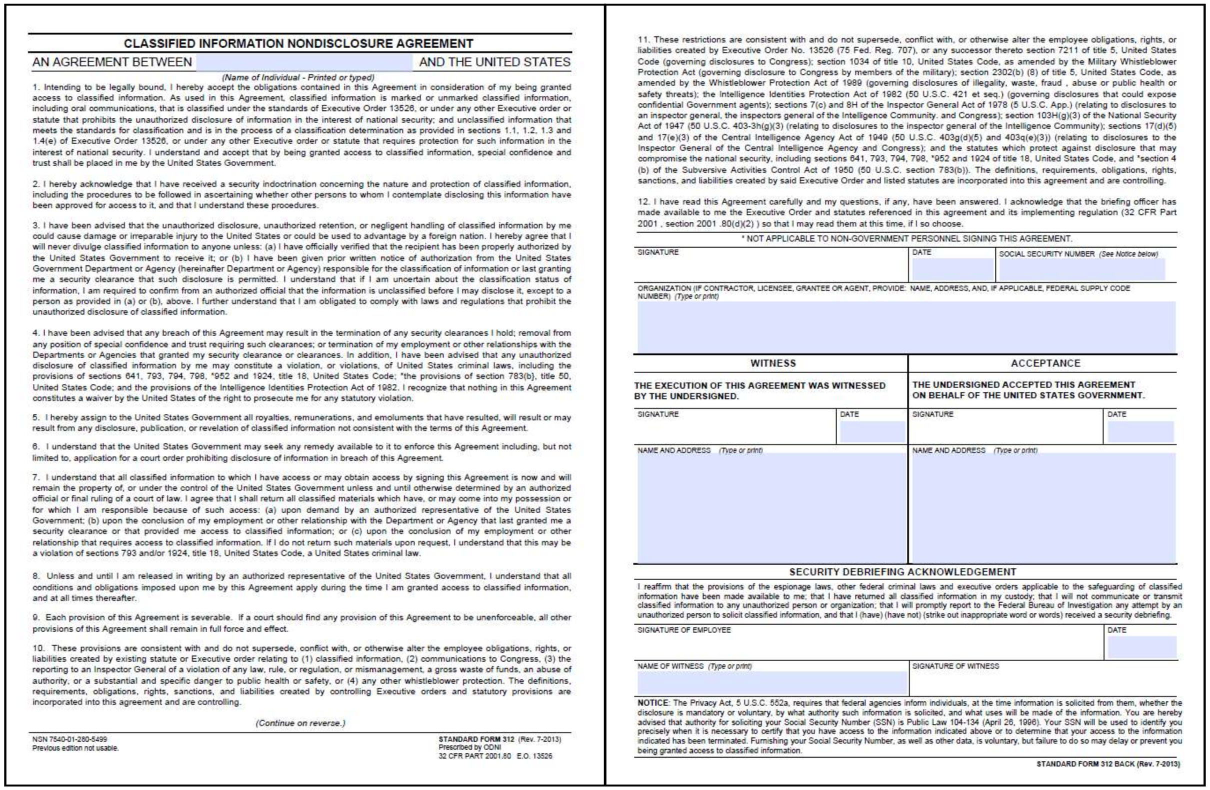
*Foreign
Influence

*Foreign Ownership, Control or Influence (FOCI) concerns

Classified Info Non-Disclosure

SF-312, Classified Information Nondisclosure Agreement

- Full Name
- SSN
- Signature
- Witness
- Debriefing
- Lifetime



CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN ______ AND THE UNITED STATES
(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 13526, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in sections 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 13526, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of sections 641, 793, 794, 798, *952 and 1924, title 18, United States Code; *the provisions of section 783(b}, title 50, United States Code; and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of sections 793 and/or 1924, title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

(Continue on reverse.)

NSN 7540-01-280-5499
Previous edition not usable.

STANDARD FORM 312 (Rev. 7-2013)
Prescribed by ODNI
32 CFR PART 2001.80 E.O. 13526

FRONT

11. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 13526 (75 Fed. Reg. 707), or any successor thereto section 7211 of title 5, United States Code (governing disclosures to Congress); section 1034 of title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); section 2302(b) (8) of title 5, United States Code, as amended by the Whistleblower Protection Act of 1989 (governing disclosures of illegality, waste, fraud , abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); sections 7(c) and 8H of the Inspector General Act of 1978 (5 U.S.C. App.) (relating to disclosures to an inspector general, the inspectors general of the Intelligence Community. and Congress); section 103H(g)(3) of the National Security Act of 1947 (50 U.S.C. 403-3h(g)(3) (relating to disclosures to the inspector general of the Intelligence Community); sections 17(d)(5) and 17(e)(3) of the Central Intelligence Agency Act of 1949 (50 U.S.C. 403g(d)(5) and 403q(e)(3)) (relating to disclosures to the Inspector General of the Central Intelligence Agency and Congress); and the statutes which protect against disclosure that may compromise the national security, including sections 641, 793, 794, 798, *952 and 1924 of title 18, United States Code, and *section 4 (b) of the Subversive Activities Control Act of 1950 (50 U.S.C. section 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

12. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulation (32 CFR Part 2001 , section 2001 .80(d)(2)) so that I may read them at this time, if I so choose.

* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

SIGNATURE	DATE	SOCIAL SECURITY NUMBER *(See Notice below)*

ORGANIZATION (IF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER) *(Type or print)*

WITNESS		**ACCEPTANCE**	
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.		**THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.**	
SIGNATURE	DATE	SIGNATURE	DATE
NAME AND ADDRESS *(Type or print)*		NAME AND ADDRESS *(Type or print)*	

SECURITY DEBRIEFING ACKNOWLEDGEMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

SIGNATURE OF EMPLOYEE	DATE
NAME OF WITNESS *(Type or print)*	SIGNATURE OF WITNESS

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Public Law 104-134 (April 26, 1996). Your SSN will be used to identify you precisely when it is necessary to certify that you have access to the information indicated above or to determine that your access to the information indicated has been terminated. Furnishing your Social Security Number, as well as other data, is voluntary, but failure to do so may delay or prevent you being granted access to classified information.

STANDARD FORM 312 BACK (Rev. 7-2013)

BACK

NOTE: Contractors Only - fill out organization information

Information Security

Information Security

The protection of classified and controlled unclassified information (CUI), including but not limited to:

- Marking
- Handling
- Transmission
- Storage
- Destruction

Information Categories

- **Classified Information**
  - TOP SECRET (TS) (Exceptionally Grave Damage)
  - SECRET (S) (Serious Damage)
  - CONFIDENTIAL (C) (Damage)

- **Controlled Unclassified Information**
  - For Official Use Only (FOUO) [FOIA exemptions 2-9]
  - Distribution Controlled
  - Personal Identifiable Information (PII)
  - Privacy Act Information
  - Proprietary Information (ownership belongs to Contractor)

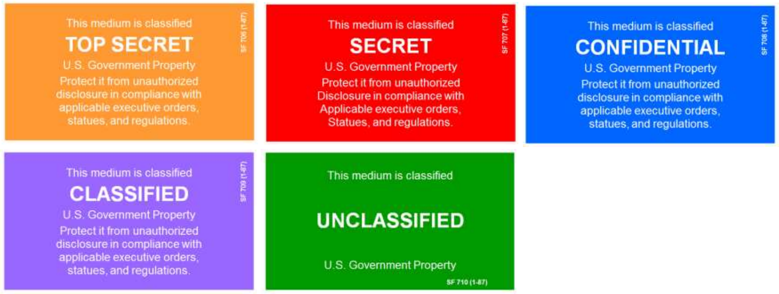
Safeguarding Classified Information

Cover Sheets

SF 703 - Top Secret (orange)
SF 704 - Secret (red)
SF 705 - Confidential (blue)

Labels

SF-706 - Top Secret (orange)
SF-707 - Secret (red)
SF-708 - Confidential (blue)
SF-709 - Classified (purple)
SF-710 - Unclassified (green)



This medium is classified
TOP SECRET
U.S. Government Property
Protect it from unauthorized disclosure in compliance with applicable executive orders, statues, and regulations.
SF 706 (1-87)

This medium is classified
SECRET
U.S. Government Property
Protect it from unauthorized Disclosure in compliance with Applicable executive orders, Statues, and regulations.
SF 707 (1-87)

This medium is classified
CONFIDENTIAL
U.S. Government Property
Protect it from unauthorized disclosure in compliance with applicable executive orders, statues, and regulations.
SF 708 (1-87)

This medium is classified
CLASSIFIED
U.S. Government Property
Protect it from unauthorized disclosure in compliance with applicable executive orders, statues, and regulations.
SF 709 (1-87)

This medium is classified
UNCLASSIFIED
U.S. Government Property
SF 710 (1-87)

Types of Classified Materials

Classified Material can include ANY of these and must be properly marked:

Machinery, Documents
Emails, Models, Faxes
Photographs, Reproductions
Storage Media, Working Papers, Meeting
Notes, Sketches, Maps, Products,
Substances,
or Materials

How Information Is Classified?

- **Original Classification**
  - Initial classification decision
  - Original Classification Authority (OCA)
    - Designated in writing by SECNAV (for Top Secret) and DUSN (Policy) (for Secret)
    - **NOTE: Commanding Officer, NSWC Carderock Division IS NOT an OCA**
- **Derivative Classification**
  - Incorporating, paraphrasing, restating, or generating, in new form, information that is already classified
  - **Training is mandatory (every two years)**
  - Derivative sources:
    - Security Classification Guide (SCG)
    - Properly marked source documents (e.g., books, pamphlets, etc.)
    - DD Form 254, DoD Contract Security Classification Specification

Classified Information Source Lines

ORIGINAL CLASSIFIER

Classified By: John Smith, Director
Reason: 1.4(c)
Declassify On: 20551231

DERIVATIVE CLASSIFIER

Classified By: Sue Jones, Code 453
Derived From: PMO Ships SCG
Declassify On: 20551231

Handling Classified Information

Must be:

- Under positive control by an authorized person and/or stored in an approved GSA container, vault, or secure room
- Discussed only in authorized areas and/or processed via authorized systems/equipment (e.g., STE, SIPRNet, JWICS)
- Protect/safeguard with appropriate cover sheet
- Properly marked
- Must have a courier card when hand carrying
- Secured/protected when found unattended

Storing Classified Information

- **Classified Information Must Be:**
  - In a GSA Approved Container/Secure Room/Vault when not being used

- **DO NOT:**
  - Leave classified material unattended
  - Leave classified material in desk drawers
  - Leave classified material in open security containers

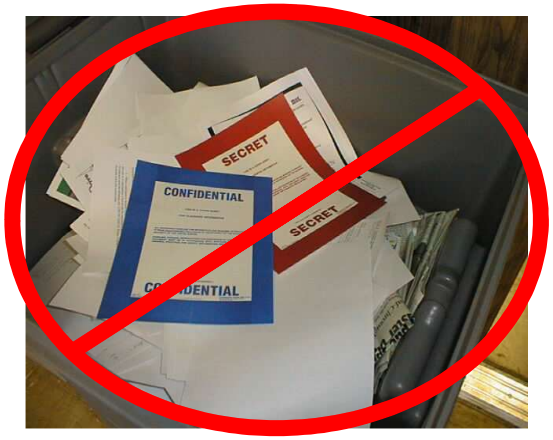
Do not take classified materials home!

<u>**DO NOT**</u> TAKE CLASSIFIED MATERIAL HOME

Destruction of Classified Information

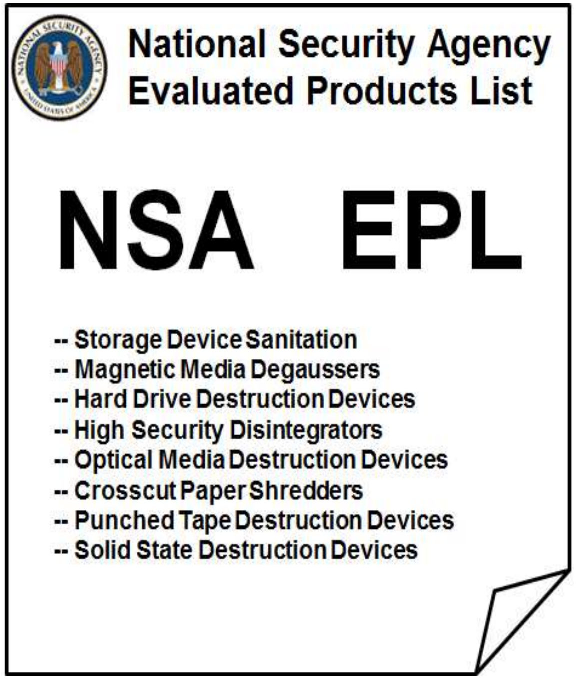
- Must be destroyed in device approved for classified material destruction*
- Approved shredders are located throughout the Command
- Shredders will contain a certification memo
- Other classified media – Contact Security (227-1408)
- All NNPI must be destroyed via approved methods*
- All purchases of classified information destruction devices must be coordinated through Security (Code 105)

Destruction device must be listed on a current NSA Evaluated Products List (EPL)



Destruction of Classified Information

- Burning
- Shredding*
- Pulverizing*
- Disintegrating*
- Degaussing*
- Pulping
- Melting
- Chemical Decomposition
- Mutilation



National Security Agency
Evaluated Products List

NSA EPL

-- Storage Device Sanitation
-- Magnetic Media Degaussers
-- Hard Drive Destruction Devices
-- High Security Disintegrators
-- Optical Media Destruction Devices
-- Crosscut Paper Shredders
-- Punched Tape Destruction Devices
-- Solid State Destruction Devices

**NSA/CSS Evaluated Products List (EPL)*

Incident Categories Defined

Willful --- Negligent --- Inadvertent

- An incident is **willful** if the person purposefully disregards DoD security or information safeguarding policies or requirements (e.g., intentionally bypassing a known security control).

- An incident is **negligent** if the person acted unreasonably in causing the spillage or unauthorized disclosure (e.g., a careless lack of attention to detail, or reckless disregard for proper procedures).

- An incident is **inadvertent** if the person did not know, and had no reasonable basis to know, that the security violation or unauthorized disclosure was occurring (e.g., the person reasonably relied on improper markings).

Per DEPSECDEF memo of 14 Aug 2014, Subject: Unauthorized Disclosure of Classified Information or Controlled Unclassified Information on DoD Information Systems

Types of Security Incidents

- **Violations** - Any knowing, willful or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information. Examples include:
  - Open/unattended security containers
  - Discussing classified information in an unsecure setting
  - Processing classified information on unclassified systems

(**Note: The presence of classified information on the NMCI NIPRNET is always considered a Security Violation).** ***[Electronic Spillage]***

- **Infractions** - Any knowing, willful or negligent action contrary to the requirements of an order or its implementing directives that do not constitute a 'violation', as defined above. Examples include:
  - Failure to use a cover sheet
  - Not using a security container checklist
  - Not using open/closed sign on a security container

Physical Security

Protection and Prevention

The two primary purposes of physical security are **PREVENTION** and **PROTECTION**. Properly designed and executed physical security programs should deter or prevent to the greatest degree possible the loss, theft, or damage to an asset.

Protection of:

- Resources
- Facilities
- Classified Information
- Operations

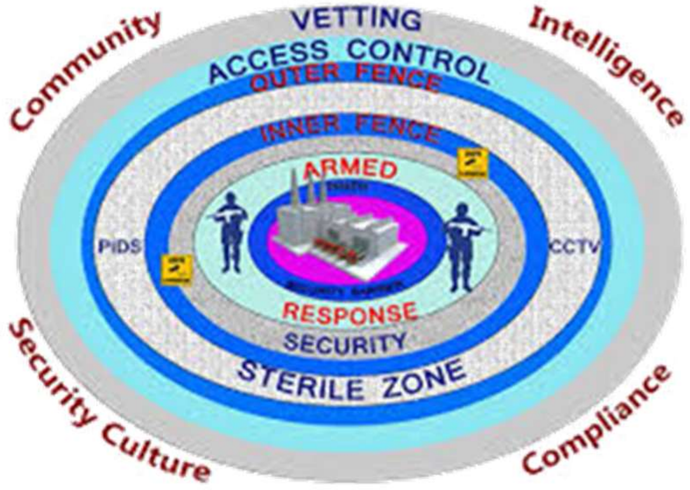
Prevention from:

- Theft
- Unauthorized Access
- Loss
- Compromise

Physical Security

Physical security functions offer security-in-depth, and include, but are not limited to:

- Perimeter fences
- Employee and visitor access controls
- Badges/Common Access Cards (CAC)
- Intrusion Detection Systems (IDS)
- Random guard patrols
- Prohibited item controls
- Entry/Exit inspections
- Visitor escorts
- CCTV monitoring



Storing Classified Information

- Custodian responsibilities
- Container maintenance
- Combo changes
- SF-700, Security Container Info
- SF-701, End of Day Checklist
- SF-702, Security Container Checklist

GSA

Security Container

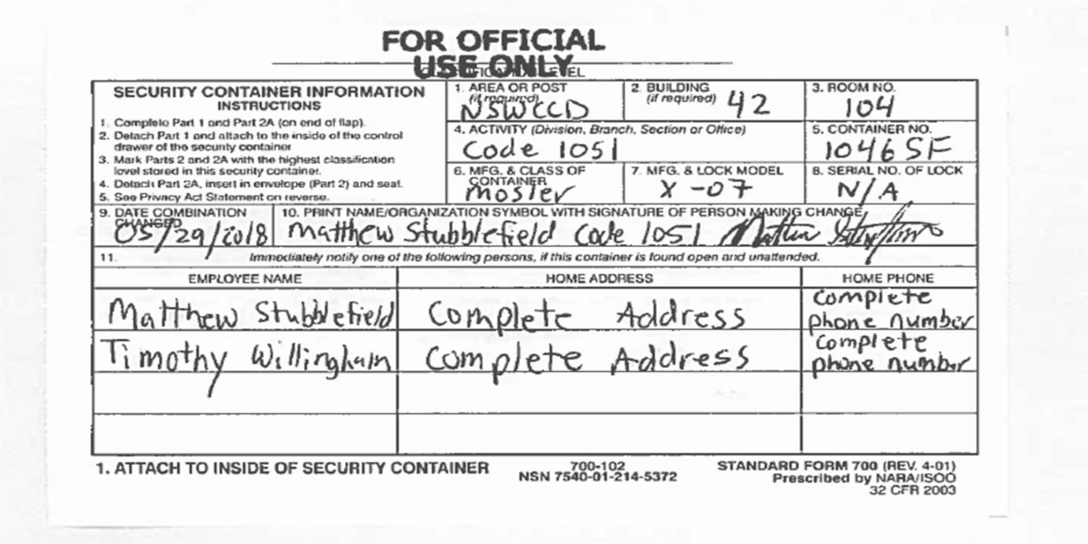
Secure Room

Vault

SF 700 Security Container Information

- Initiate a combination change when an employee no longer requires access, if there is a compromise, and/or when a container is placed in/out of service.

- Fill out page one and place in an opaque envelope
  - Lists after-hours custodian contact information (PII)
  - Place sealed envelop in control drawer of security container
  - Page two lists combo, place in sealed envelope and provide to Security Office



FOR OFFICIAL USE ONLY

SECURITY CONTAINER INFORMATION
INSTRUCTIONS

1. Complete Part 1 and Part 2A (on end of flap).
2. Detach Part 1 and attach to the inside of the control drawer of the security container
3. Mark Parts 2 and 2A with the highest classification level stored in this security container.
4. Detach Part 2A, insert in envelope (Part 2) and seal.
5. See Privacy Act Statement on reverse.

1. AREA OR POST (if required): NSWCCD
2. BUILDING (if required): 42
3. ROOM NO.: 104
4. ACTIVITY (Division, Branch, Section or Office): Code 1051
5. CONTAINER NO.: 1046SF
6. MFG. & CLASS OF CONTAINER: Mosler
7. MFG. & LOCK MODEL: X-07
8. SERIAL NO. OF LOCK: N/A
9. DATE COMBINATION CHANGED: 05/29/2018
10. PRINT NAME/ORGANIZATION SYMBOL WITH SIGNATURE OF PERSON MAKING CHANGE: Matthew Stubblefield Code 1051

11. *Immediately notify one of the following persons, if this container is found open and unattended.*

EMPLOYEE NAME	HOME ADDRESS	HOME PHONE
Matthew Stubblefield	Complete Address	complete phone number
Timothy Willingham	Complete Address	complete phone number

1. ATTACH TO INSIDE OF SECURITY CONTAINER

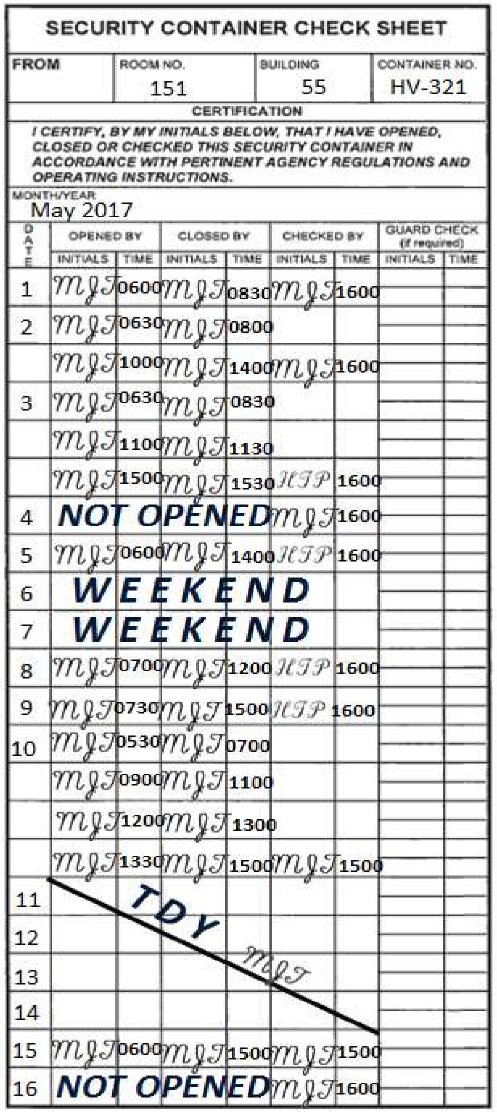
700-102
NSN 7540-01-214-5372

STANDARD FORM 700 (REV. 4-01)
Prescribed by NARA/ISOO
32 CFR 2003

Security Containers and Secure Rooms

- SF 702-Security Container Check Sheet
  - Posted on outside of container or door
  - Every day must be accounted for including weekends and holidays
  - Completed form retained for 90 days from last entry

NOSTALGIA IS WISHING YOU HAD CHECKED YOUR SAFE TWICE TO MAKE SURE IT WAS LOCKED.



SECURITY CONTAINER CHECK SHEET

FROM	ROOM NO.	BUILDING	CONTAINER NO.
	151	55	HV-321

CERTIFICATION

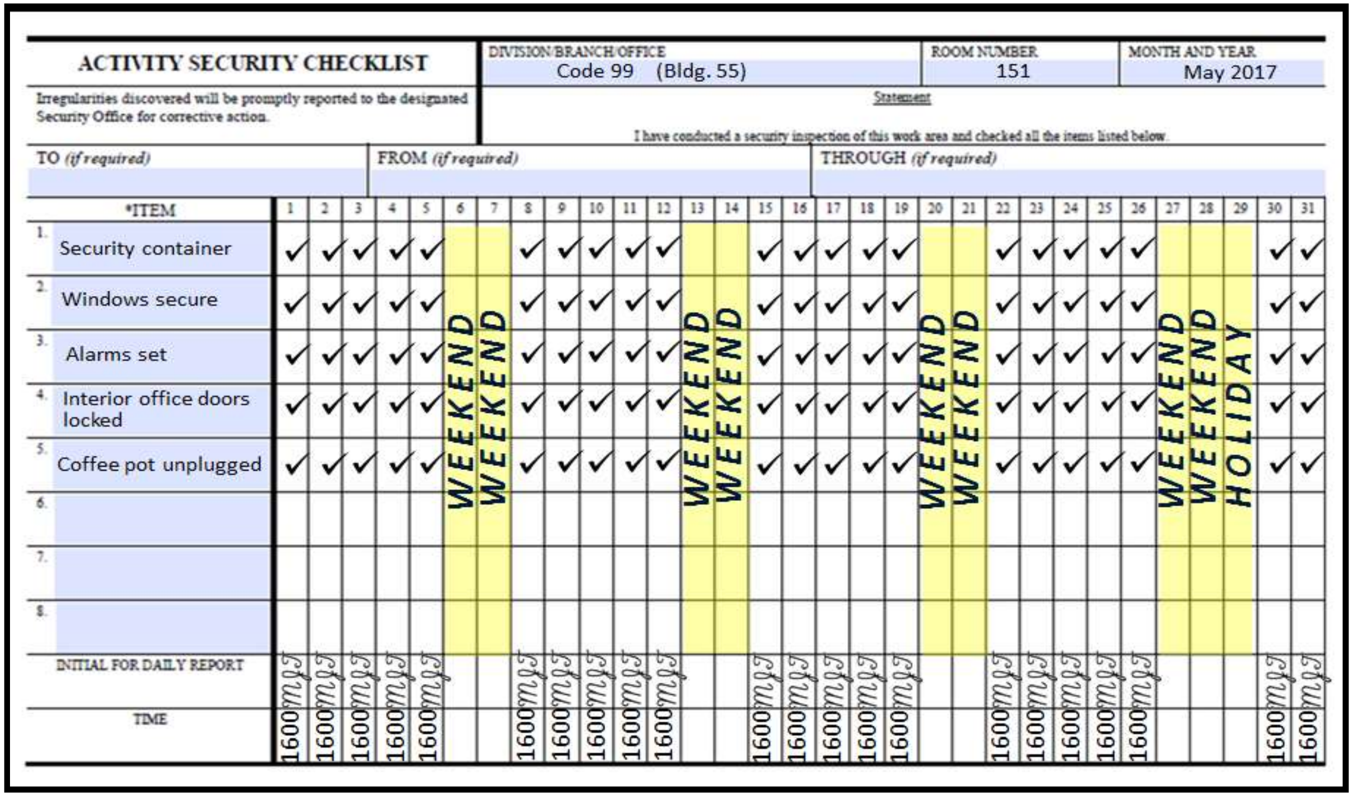
I CERTIFY, BY MY INITIALS BELOW, THAT I HAVE OPENED, CLOSED OR CHECKED THIS SECURITY CONTAINER IN ACCORDANCE WITH PERTINENT AGENCY REGULATIONS AND OPERATING INSTRUCTIONS.

MONTH/YEAR
May 2017

DATE	OPENED BY		CLOSED BY		CHECKED BY		GUARD CHECK (if required)	
	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME	INITIALS	TIME
1	MJT	0600	MJT	0830	MJT	1600		
2	MJT	0630	MJT	0800				
	MJT	1000	MJT	1400	MJT	1600		
3	MJT	0630	MJT	0830				
	MJT	1100	MJT	1130				
	MJT	1500	MJT	1530	HTP	1600		
4	NOT OPENED				MJT	1600		
5	MJT	0600	MJT	1400	HTP	1600		
6	WEEKEND							
7	WEEKEND							
8	MJT	0700	MJT	1200	HTP	1600		
9	MJT	0730	MJT	1500	HTP	1600		
10	MJT	0530	MJT	0700				
	MJT	0900	MJT	1100				
	MJT	1200	MJT	1300				
	MJT	1330	MJT	1500	MJT	1500		
11	TDY							
12								
13					MJT			
14								
15	MJT	0600	MJT	1500	MJT	1500		
16	NOT OPENED				MJT	1600		

End-of-Day Security Checks

- SF 701-Activity Security Checklist
  - Posted on inside of room, closest to exit
  - Annotate weekends and holidays
  - Completed form retained for 90 days from last day



ACTIVITY SECURITY CHECKLIST

DIVISION/BRANCH/OFFICE: Code 99 (Bldg. 55)

ROOM NUMBER: 151

MONTH AND YEAR: May 2017

Irregularities discovered will be promptly reported to the designated Security Office for corrective action.

Statement

I have conducted a security inspection of this work area and checked all the items listed below.

TO *(if required)*

FROM *(if required)*

THROUGH *(if required)*

*ITEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1. Security container	✓	✓	✓	✓	✓	WEEKEND	WEEKEND	✓	✓	✓	✓	✓	WEEKEND	WEEKEND	✓	✓	✓	✓	✓	WEEKEND	WEEKEND	✓	✓	✓	✓	✓	WEEKEND	WEEKEND	HOLIDAY	✓	✓
2. Windows secure	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓	✓				✓	✓
3. Alarms set	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓	✓				✓	✓
4. Interior office doors locked	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓	✓				✓	✓
5. Coffee pot unplugged	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓	✓				✓	✓
6.																															
7.																															
8.																															
INITIAL FOR DAILY REPORT	mjT	mjT	mjT	mjT	mjT			mjT	mjT	mjT	mjT	mjT			mjT	mjT	mjT	mjT	mjT			mjT	mjT	mjT	mjT	mjT				mjT	mjT
TIME	1600	1600	1600	1600	1600			1600	1600	1600	1600	1600			1600	1600	1600	1600	1600			1600	1600	1600	1600	1600				1600	1600

Access

- Base Access:
  - Common Access Card (CAC)
  - Authorized pass
  - Defense Biometric Identification System (DBIDS)
    - Credentialing for contractors, vendors, and suppliers requiring recurring access
    - Not required for contractors with CAC
    - All contractors (w/o a CAC), vendors and delivery personnel are required to complete and sign the SECNAV Form 5512/1
    - Credentials require a sponsor

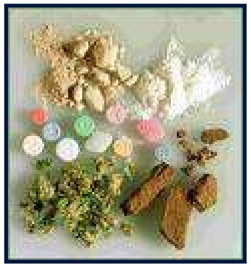
Prohibited Items

Theses items and those similar in nature are **prohibited** inside NSWCCD Office Spaces

*** Photography**

Alcohol

Drugs



XXX

Sexually Explicit Material

Weapons (Guns/Knives)

*Permission Required

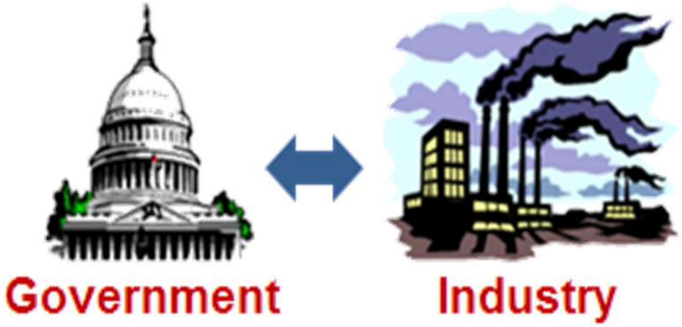
Cell Phones and PED Policy

- **Personally-owned cell phones are prohibited in:**
  - Restricted Areas
  - Open Storage Areas
  - Sensitive Compartmented Information Facilities (SCIF)
  - Explosive operations buildings and storage areas
- **CUI**
  - NAVSEA and Carderock PED Policies in place
    - NAVSEA Update, May 2016: "In such spaces [basic office spaces], sound judgment is required prior to conducting discussions. Although PEDs are authorized in these locations, each employee is responsible to ensure that controlled information is not inadvertently exposed to unauthorized personnel and recording of any kind is prohibited."

Industrial Security

Industrial Security

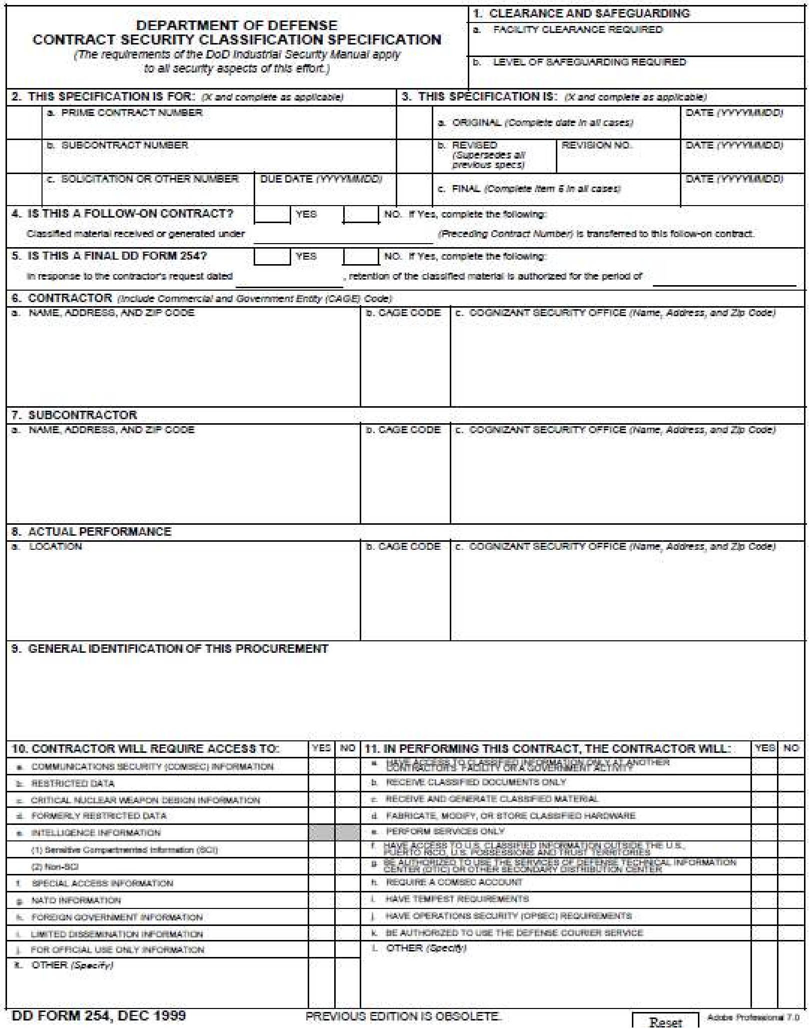
- A partnership between the federal gov't and industry in order to safeguard classified information
- Establishes standards for contracting companies who have access to classified information
- Prevents unauthorized disclosure of classified by:
  -- Defining requirements
  -- Identifying restrictions
  -- Establishing safeguards



Contractors and Classified Info

- Prior to disclosing classified information:
  - ➢ Determine if contractor requires access in connection with a legitimate U. S. Government requirement
    - Contract Solicitation
    - Pre-contract Negotiation
    - Contractual Relationship
    - IR&D Effort
  - ➢ Determination based on:
    - Facility clearance valid for access at same or lower classification level as FCL
    - Storage capability

DD Form 254



DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION
(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING
a. FACILITY CLEARANCE REQUIRED
b. LEVEL OF SAFEGUARDING REQUIRED

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*
a. PRIME CONTRACT NUMBER
b. SUBCONTRACT NUMBER
c. SOLICITATION OR OTHER NUMBER | DUE DATE *(YYYYMMDD)*

3. THIS SPECIFICATION IS: *(X and complete as applicable)*
a. ORIGINAL *(Complete date in all cases)* | DATE *(YYYYMMDD)*
b. REVISED *(Supersedes all previous specs)* | REVISION NO. | DATE *(YYYYMMDD)*
c. FINAL *(Complete Item 5 in all cases)* | DATE *(YYYYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? □ YES □ NO. If Yes, complete the following:
Classified material received or generated under ____________ *(Preceding Contract Number)* is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? □ YES □ NO. If Yes, complete the following:
In response to the contractor's request dated ____________, retention of the classified material is authorized for the period of ____________

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*
a. NAME, ADDRESS, AND ZIP CODE | b. CAGE CODE | c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

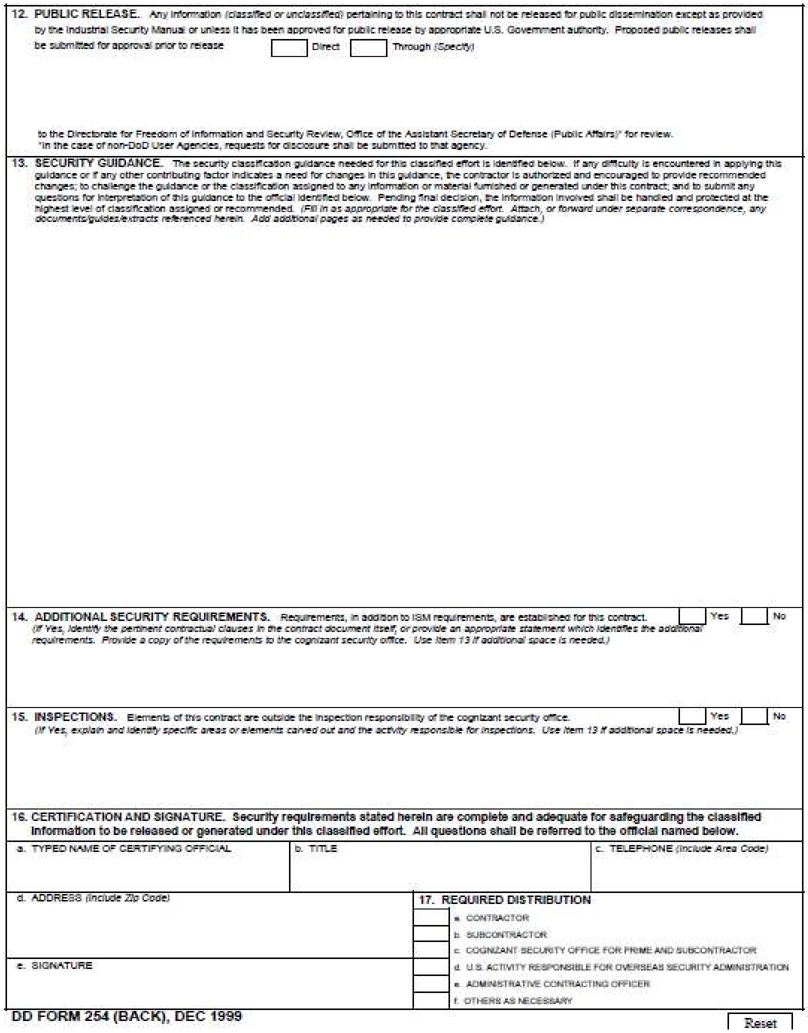
7. SUBCONTRACTOR
a. NAME, ADDRESS, AND ZIP CODE | b. CAGE CODE | c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

8. ACTUAL PERFORMANCE
a. LOCATION | b. CAGE CODE | c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION			a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		
b. RESTRICTED DATA			b. RECEIVE CLASSIFIED DOCUMENTS ONLY		
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION			c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		
d. FORMERLY RESTRICTED DATA			d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		
e. INTELLIGENCE INFORMATION	▨	▨	e. PERFORM SERVICES ONLY		
(1) Sensitive Compartmented Information (SCI)			f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		
(2) Non-SCI			g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		
f. SPECIAL ACCESS INFORMATION			h. REQUIRE A COMSEC ACCOUNT		
g. NATO INFORMATION			i. HAVE TEMPEST REQUIREMENTS		
h. FOREIGN GOVERNMENT INFORMATION			j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		
i. LIMITED DISSEMINATION INFORMATION			k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		
j. FOR OFFICIAL USE ONLY INFORMATION			l. OTHER *(Specify)*		
k. OTHER *(Specify)*					

DD FORM 254, DEC 1999 PREVIOUS EDITION IS OBSOLETE. Reset Adobe Professional 7.0



12. PUBLIC RELEASE. Any information *(classified or unclassified)* pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release □ Direct □ Through *(Specify)*

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)*

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. □ Yes □ No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. □ Yes □ No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.
a. TYPED NAME OF CERTIFYING OFFICIAL | b. TITLE | c. TELEPHONE *(Include Area Code)*
d. ADDRESS *(Include Zip Code)*
e. SIGNATURE

17. REQUIRED DISTRIBUTION
□ a. CONTRACTOR
□ b. SUBCONTRACTOR
□ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
□ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
□ e. ADMINISTRATIVE CONTRACTING OFFICER
□ f. OTHERS AS NECESSARY

DD FORM 254 (BACK), DEC 1999 Reset

Other General Security Tasks

Other Key Processes

- Base Access for Visitors
- Hosting Foreign Visitors
- Foreign Travel Process

NSWCCD Visitors

- Major events (e.g., sub races, STEM competition)
  - Visitors are required to complete and sign the SECNAV Form 5512/1
  - Form 5512/1 must be submitted five (5) days prior to visit
- Classified Meetings or other official visits
  - Carderock employee notifies Security Office of visitor
  - Initiate coordination at least 10 days prior to visit
- Upon arrival Visitor must provide name of POC

Hosting Foreign Visitors

- Official Visits
  - Must be processed/approved via Foreign Visit System (FVS)
  - Security Division notifies Code sponsor and NCIS (Contact Officer)
  - Three types: One time; Recurring; Extended
  - Coordinate with NAVSEA HQ if DDL required
  - If authorized, visitor can have accessed to classified information
- Unofficial Visits
  - Courtesy calls, general visits, public events, etc.
  - Hosting code submits CARDEROCKDIV 5512/6
  - Security Division will coordinate with host code and Visitor Center
  - No access to classified information is authorized

Foreign Travel

All personnel traveling outside of U.S. on official duty or on leisure must:

- Submit a CARDERDIV Form 5540/1 at least 30 days prior to departure
- Submit a CARDERDIV Form 5540/2 within 3 business days of return to duty

Pre-travel guidance is provided in the Foreign Clearance Guide (https://www.fcg.pentagon.mil)

This process ensures the Foreign Travel Brief is given to personnel who require them. The briefs increase awareness regarding:

- Personal Safety
- Potential targeting
- Travel warnings and alerts
- Where to seek assistance

Check-In/Check-Out Procedures

***ALL* personnel *MUST* check-in and check-out with the Security Division (Code 105)**

- Receive Security Briefings/Debriefings
- Turn in badges, credentials, CACs, ID Cards, etc.
- Receive/Return Courier Cards
- Update JPAS records
- Ensure ALL classified information assigned to you is transferred to the appropriate program/person before check-out
- **Security (Code 105), Bldg. 42 should be the final stop, on the last duty day, before departing the installation.**

Summary

Summary

Why are we here?

Ana Montes

Edward Snowden

Jerry Whitworth

Aldrich Ames

Robert Hanssen

Bradley Manning

The importance of security awareness and vigilance on the part of all employees cannot be overemphasized. It helps to detect internal and external threats and vulnerabilities ultimately assisting in preventing security breaches. It is only when all employees are vigilant and aware, that those who disregard security policies and procedures can be identified before causing irreparable damage to national security.

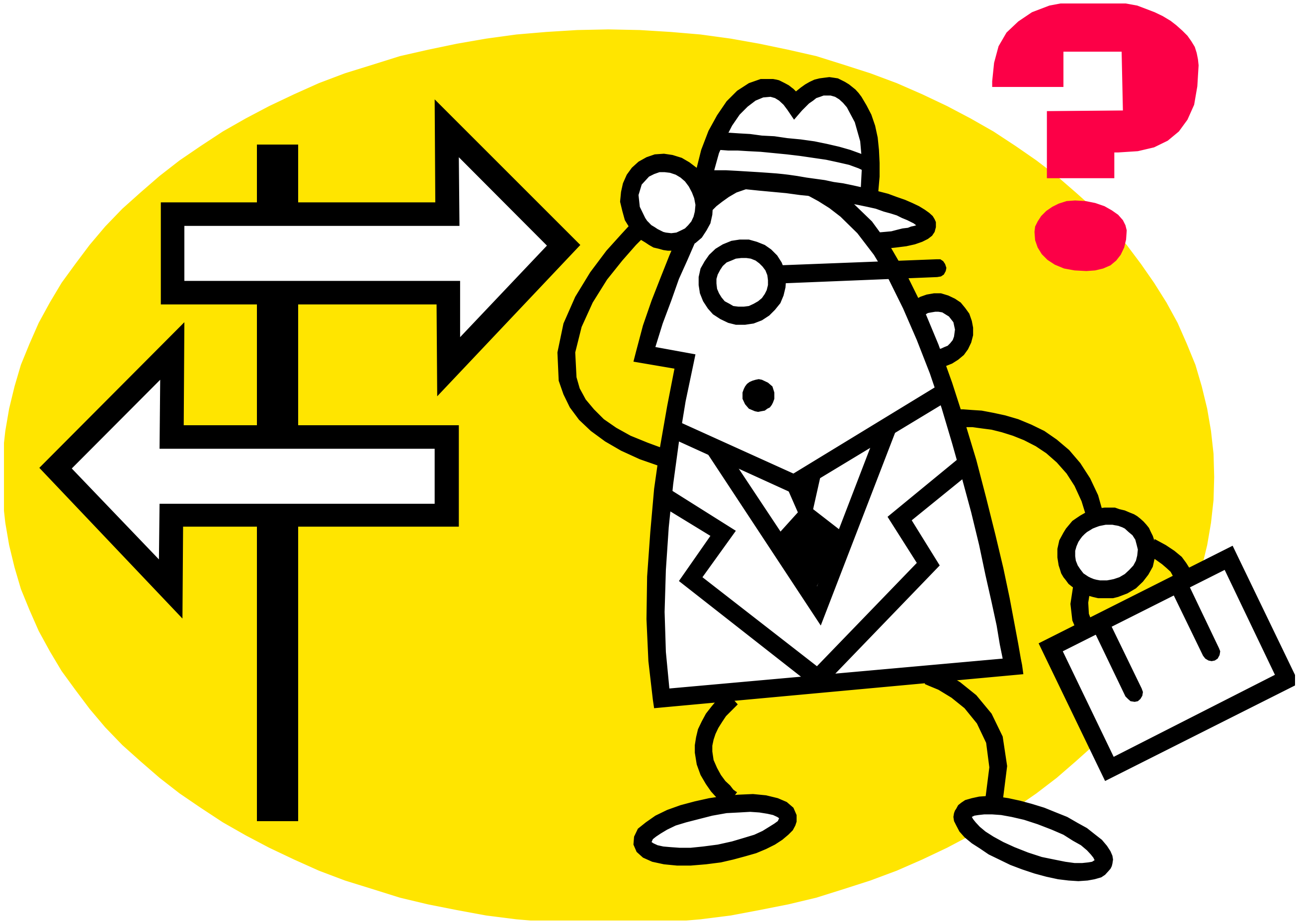
Security Is…

» You
» Me
» Us
» We

….a Team effort.

…..and Everyone’s Responsibility

Questions



Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE

Controlled Unclassified Information (CUI)

Vicky Davis, Security Policy and Programs (Code 1051)

NAVSEA
WARFARE CENTERS
Carderock

Captain Todd E. Hutchison
Commanding Officer, NSWCCD

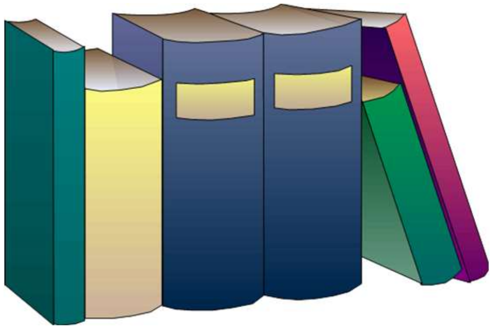
Larry Tarasek
Technical Director, NSWCCD

Controlled Unclassified Information (CUI)

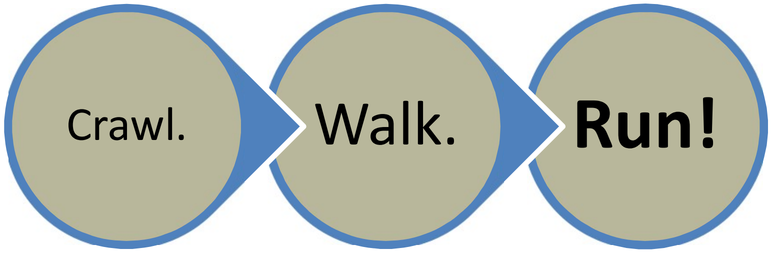
Defined as information that requires safeguarding or dissemination controls pursuant to and consistent with applicable Law, Regulations, and Government-Wide Policies (LRGWP) but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. CUI has its own Executive Order – 13556.

The originator of a document is responsible for determining, at origination, whether the information may qualify for CUI status, and if so, for applying the appropriate CUI markings.

CUI Policy/Resources



- Executive Order 13556
- 32 CFR Part 2002
- DoDI 5200.48
- DoD CUI Registry: https://www.dodcui.mil/Home/DoD-CUI-Registry/
- NSWCCD CUI Desk Guide:
  Will soon be published on Cuthill site.
- Training - TWMS #686564 - "DoD Mandatory Controlled Unclassified Information (CUI) Training"



Crawl. Walk. Run!

NSWCCD is currently in a "Crawl stage" of a phased NAVSEA implementation plan and not all CUI policy, markings, and training modules are being implemented at this time.

Categories of CUI

Category	Description
Agriculture	Agricultural operation, farming or conservation practices, or the actual land.
Controlled Technical Information*	Information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.
Copyright	A form of protection provided by the laws of the United States (17 USC) to the authors of "original works of authorship."
Critical Infrastructure*	The most vital systems and assets (whether physical or virtual), who's incapacity or destruction would have a debilitating impact on the nation's security, economy, and/or public safety.
Emergency Management	Information concerning the continuity of executive branch operations during all-hazards emergencies or other situations that may disrupt normal operations.
Export Control*	Unclassified information concerning certain items, commodities, technology, software, or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives.
Financial*	Related to the duties, transactions, or otherwise falling under the purview of financial institutions or United States Government fiscal functions.
Foreign Government Information*	Information provided by, otherwise made available by, or produced in cooperation with, a foreign government or international organization.
Geodetic Product Information	Related to imagery, imagery intelligence, or geospatial information.
Immigration	Related to admission of non-US citizens into the United States and applications for temporary and permanent residency.

Categories of CUI

Category	Description
Information Systems Vulnerability Information	Related to information that if not protected, could result in adverse effects to information systems.
Intelligence	Related to intelligence activities, sources, or methods.
Law Enforcement	Related to techniques and procedures for law enforcement operations, investigations, prosecutions, or enforcement actions.
Legal	Information related to proceedings in judicial or quasi-judicial settings.
North Atlantic Treaty Organization (NATO)	Related to information generated by NATO member countries under the North Atlantic Treaty international agreement, signed on April 4, 1949.
Nuclear*	Related to protection of information concerning nuclear reactors, materials, or security.
Patent	Patent is a property right granted by the Government of the United States of America to an inventor "to exclude others profiting off of or benefiting from the patent owner’s property.”
Privacy	Personal information, or, in some cases, "personally identifiable information," as defined in OMB M-07-16, or "means of identification" as defined in 18 USC 1028(d)(7).
Proprietary Business Information*	Material and information relating to, or associated with, a company's products, business, or activities; data or statements; trade secrets; product R&D; and performance specifications, etc.
SAFETY Act Information	The regulations implementing the Support Anti-terrorism by Fostering Effective Technologies Act of 2002.

Freedom of Information Act (FOIA)

- Informs the public of information while appropriately protecting government interests
- Provides individuals with access to many types of records that are exempt from access under the Privacy Act of 1974

Promotes transparency & accountability

Dissemination controls are applied for information that may be withheld from the public if disclosure would reasonably be expected to cause a foreseeable harm to an interest protected under Exemptions 2 through 9 of the FOIA.

FOIA Exemptions

Number	Description
Exemption 2	Information that pertains solely to the internal rules and practices of the agency that, if released, would allow circumvention of an agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission.
Exemption 3	Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.
Exemption 4	Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company.
Exemption 5	Inter- or intra-agency memorandums or letters containing information considered privileged in civil litigation. (Examples: decision making processes and attorney-client privilege.)
Exemption 6	Information, the release of which would reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.
Exemption 7	Records or information compiled for law enforcement purposes that: (a) Could reasonably be expected to interfere with law enforcement proceedings. (b) Would deprive a person of a right to a fair trial or impartial adjudication. (c) Could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others. (d) Disclose the identity of a confidential source. (e) Disclose investigative techniques and procedures. (f) Could reasonably be expected to endanger the life or physical safety of any individual.
Exemption 8	Certain records of agencies responsible for supervision of financial institutions.
Exemption 9	Geological and geophysical information (including maps) concerning wells.

Why CUI?

- Mixed bag of agency inconsistencies
- Old legacy/ad hoc markings no longer used (not a complete list):

"For Official Use Only" or "FOUO"

"Sensitive But Unclassified" or "SBU"

"Unclassified Controlled Nuclear Information" or "UCNI"

"Law Enforcement Sensitive", "LES"

"Limited Distribution" or "LIMDIS"

- Legacy markings have been phased out. Mark all new documents and emails containing CUI with "CUI"

➢ Existing legacy documents do <u>not</u> need to be remarked at this time, as long as they remain under DoD control or are accessed online/downloaded for use within the DoD.

CONTROLLED UNCLASSIFIED INFORMATION
REPLACES "FOR OFFICIAL USE ONLY" DESIGNATION
FOUO
CUI
APPROVED

Marking CUI

We are in a NAVSEA “Crawl” phase of a “Crawl, Walk, Run” implementation plan. For now, ONLY:

1. Mark CUI documents/emails with the banner marking of “(CUI)” at the top and bottom of the page/email.
2. Include a “CUI Designation Indicator” on the bottom right side of the first page/cover of the document, above the CUI footer banner. Example:
    - Controlled by: Department of the Navy (always this for now)
    - Controlled by: NSWCCD Code 105 (agency/office/code making the determination)
    - CUI Category: OPSEC, PHYS (from the DoD CUI Registry @ https://www.dodcui.mil)
    - Distribution/Dissemination Control: FEDCON (Distribution statements B-F or other LDCs)
    - POC: John Doe, john.doe@navy.mil, 301-555-5555 (originator/authorized CUI holder)

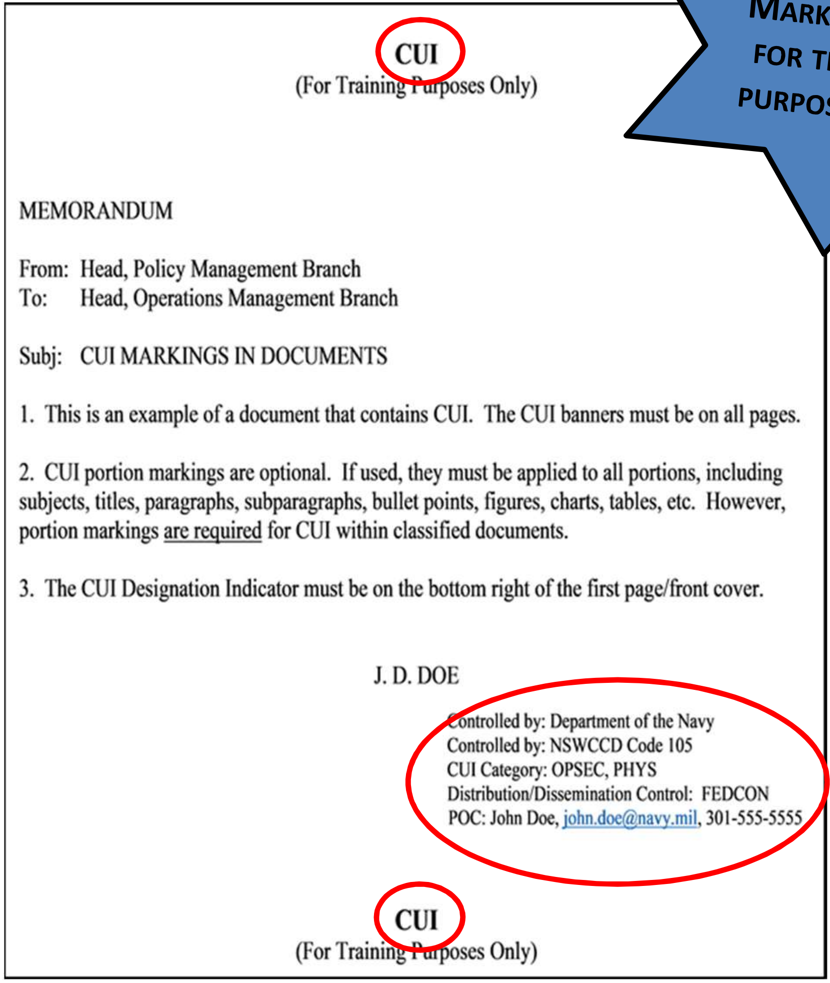
PORTION MARKINGS

- Optional in the Crawl phase. If used, they must be applied to all portions, including subjects, titles, paragraphs, bullet points, figures, charts, tables, etc.
- Required for CUI within classified documents

CUI Marking Examples

- ✓ Banner markings top/bottom
- ✓ Designation Indicator on right

MARKINGS ARE FOR TRAINING PURPOSES ONLY



CUI
(For Training Purposes Only)

MEMORANDUM

From: Head, Policy Management Branch
To: Head, Operations Management Branch

Subj: CUI MARKINGS IN DOCUMENTS

1. This is an example of a document that contains CUI. The CUI banners must be on all pages.

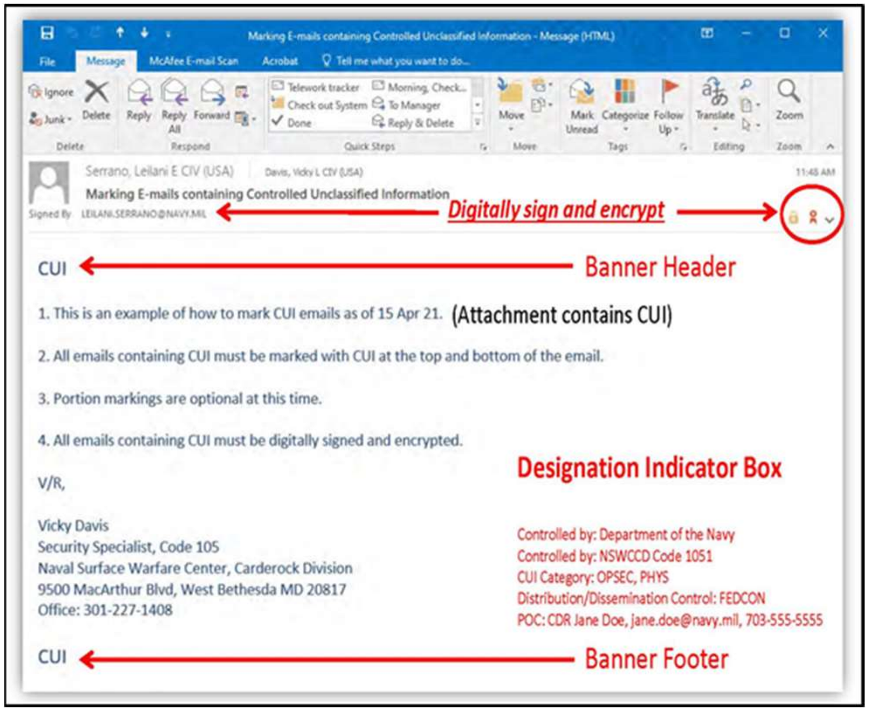
2. CUI portion markings are optional. If used, they must be applied to all portions, including subjects, titles, paragraphs, subparagraphs, bullet points, figures, charts, tables, etc. However, portion markings <u>are required</u> for CUI within classified documents.

3. The CUI Designation Indicator must be on the bottom right of the first page/front cover.

J. D. DOE

Controlled by: Department of the Navy
Controlled by: NSWCCD Code 105
CUI Category: OPSEC, PHYS
Distribution/Dissemination Control: FEDCON
POC: John Doe, john.doe@navy.mil, 301-555-5555

CUI
(For Training Purposes Only)



Serrano, Leilani E CIV (USA) | Davis, Vicky L CIV (USA) 11:48 AM
Marking E-mails containing Controlled Unclassified Information
Signed By LEILANI.SERRANO@NAVY.MIL

Digitally sign and encrypt

CUI

Banner Header

1. This is an example of how to mark CUI emails as of 15 Apr 21. (Attachment contains CUI)

2. All emails containing CUI must be marked with CUI at the top and bottom of the email.

3. Portion markings are optional at this time.

4. All emails containing CUI must be digitally signed and encrypted.

V/R,

Vicky Davis
Security Specialist, Code 105
Naval Surface Warfare Center, Carderock Division
9500 MacArthur Blvd, West Bethesda MD 20817
Office: 301-227-1408

Designation Indicator Box

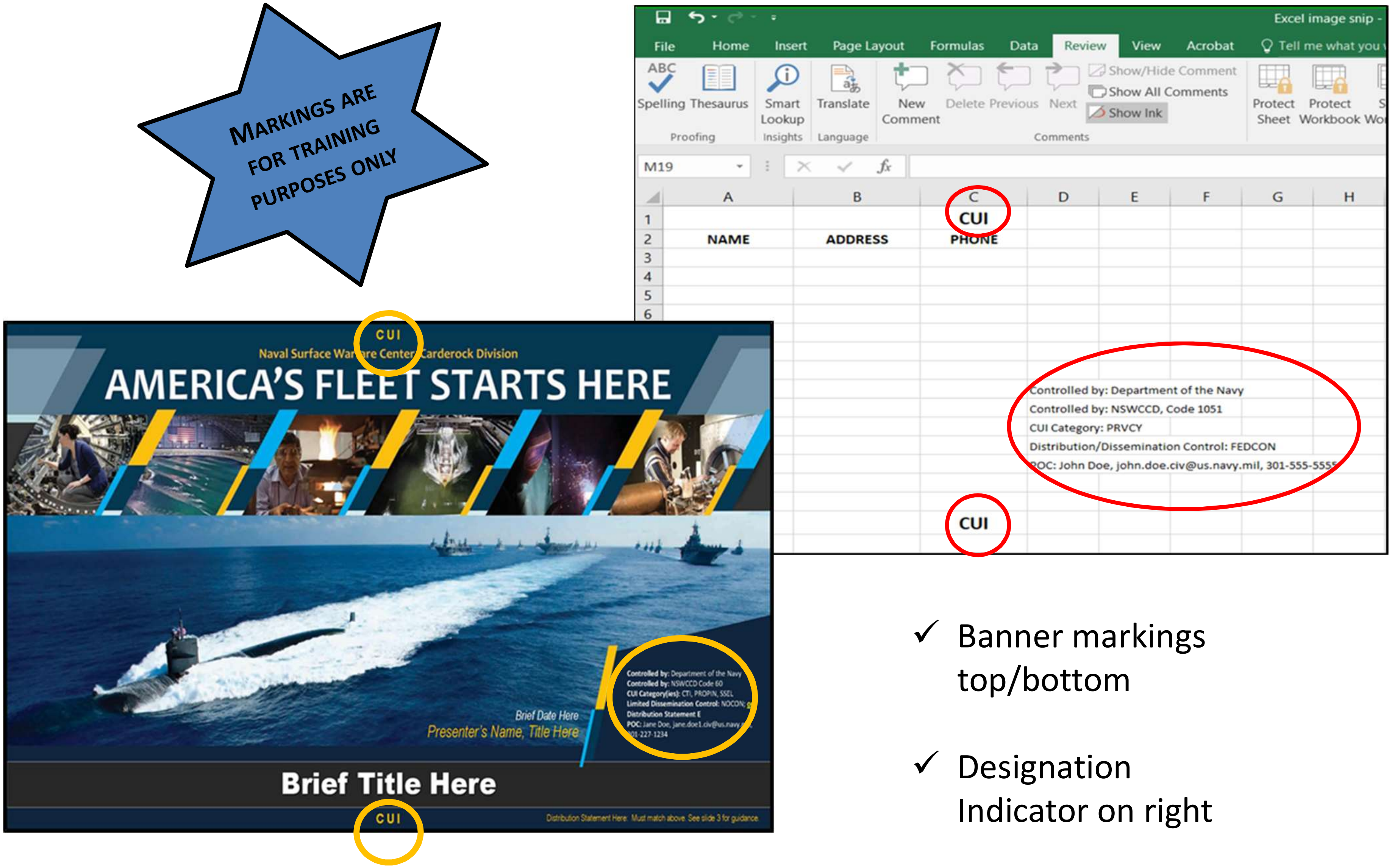
Controlled by: Department of the Navy
Controlled by: NSWCCD Code 1051
CUI Category: OPSEC, PHYS
Distribution/Dissemination Control: FEDCON
POC: CDR Jane Doe, jane.doe@navy.mil, 703-555-5555

CUI

Banner Footer

CUI Marking Examples

MARKINGS ARE FOR TRAINING PURPOSES ONLY



CUI

NAME	ADDRESS	PHONE

Controlled by: Department of the Navy
Controlled by: NSWCCD, Code 1051
CUI Category: PRVCY
Distribution/Dissemination Control: FEDCON
POC: John Doe, john.doe.civ@us.navy.mil, 301-555-5555

CUI

CUI

Naval Surface Warfare Center Carderock Division

AMERICA'S FLEET STARTS HERE

Brief Date Here
Presenter's Name, Title Here

Controlled by: Department of the Navy
Controlled by: NSWCCD Code 60
CUI Category(ies): CTI, PROPIN, SSEL
Limited Dissemination Control: NOCON;
Distribution Statement E
POC: Jane Doe, jane.doe1.civ@us.navy.
301-227-1234

Brief Title Here

CUI

Distribution Statement Here. Must match above. See slide 3 for guidance.

- ✓ Banner markings top/bottom
- ✓ Designation Indicator on right

Distribution Statements/Controls

Distribution Statements on Technical Documents –

"Statements intended to facilitate control, secondary distribution, and release of these documents without the need to repeatedly obtain approval or authorization from the controlling DoD office."

A: Approved for public release, distribution is unlimited
B: Distribution authorized to U.S. Government agencies only
C: Distribution authorized to U.S. Government agencies/their contractors
D: Distribution authorized to DoD & U.S. DoD contractors only
E: Distribution authorized to DoD components only
F: Further distribution as directed by the Controlling Authority
X: Use of Distro X is superseded [Convert to Distro C, w/ Export Control]

Distribution Statement "Reasons"

- Public Release
- Administrative or Operational Use
- Contractor Performance Evaluation
- Critical Technology
- Export Controlled
- Foreign Government Information
- Operations Security

TECHNICAL DOCUMENTS

- Premature Dissemination
- Proprietary Information
- Test and Evaluation
- Direct Military Support
- Software Documentation
- Specific Authority
- Vulnerability Information

REFERENCE: DODI 5230.24

Distribution Statements/Controls

NAVSEA WARFARE CENTERS Carderock Division

Controlled Technical Information (CTI) is a category of CUI

For use on technical documents only (not administrative or general correspondence)

All newly created, revised, or previously unmarked classified and unclassified DoD technical documents must be assigned a distribution statement

Document authors/controlling DoD offices are responsible for initial distribution control determinations/reasons

Wording may not be modified to specify additional distribution

Removal of or tampering with control markings by unauthorized personnel is strictly prohibited

Must remain in effect until changed or removed by the controlling office

Export-controlled data must be marked with applicable export-control statement

YOU are the Subject Matter Expert (SME)!!

Safeguarding CUI

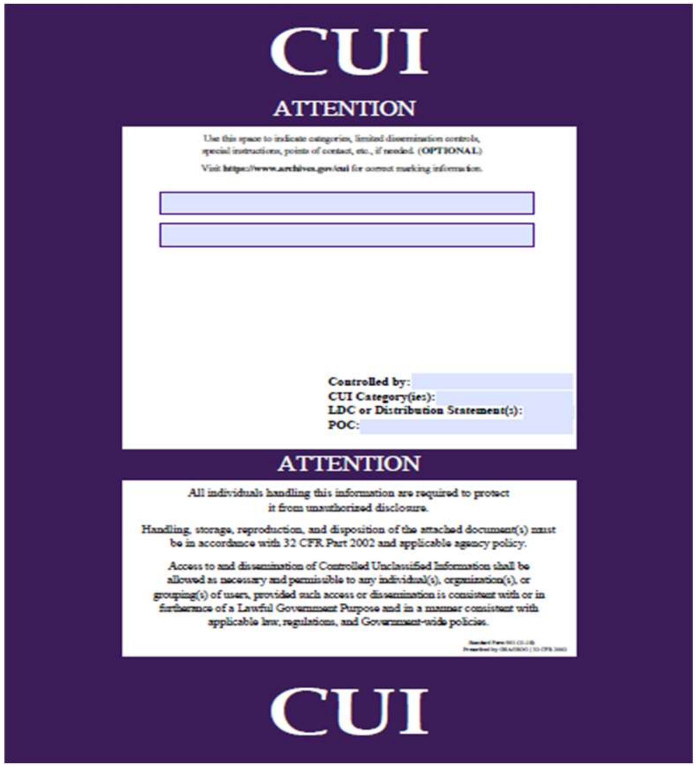
✓ DO'S

- Be mindful of CUI, viewable/audible, in background/environment when participating on web-based collaboration platforms
- Digitally sign and encrypt all e-mails containing CUI
- Use cover sheets and media labels
- Use First Class Mail; Fax; Parcel Post
- Obtain approval prior to public release

✗ DON'TS

- Discuss CUI on personal devices
- Process or store CUI on personal computers
- Post CUI on public websites or social media platforms

CUI Cover Sheets/Media Labels



CUI

ATTENTION

Use this space to indicate categories, limited dissemination controls, special instructions, points of contact, etc., if needed. (**OPTIONAL**)

Visit **https://www.archives.gov/cui** for correct marking information.

Controlled by:
CUI Category(ies):
LDC or Distribution Statement(s):
POC:

ATTENTION

All individuals handling this information are required to protect it from unauthorized disclosure.

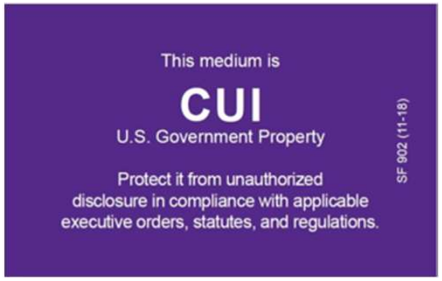
Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR Part 2002 and applicable agency policy.

Access to and dissemination of Controlled Unclassified Information shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.

Standard Form 901 (11-18)
Prescribed by GSA/ISOO | 32 CFR 2002

CUI

SF 901
Cover Sheet

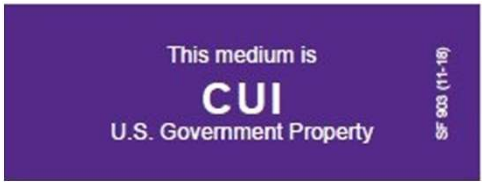


This medium is
CUI
U.S. Government Property

Protect it from unauthorized disclosure in compliance with applicable executive orders, statutes, and regulations.

SF 902 (11-18)

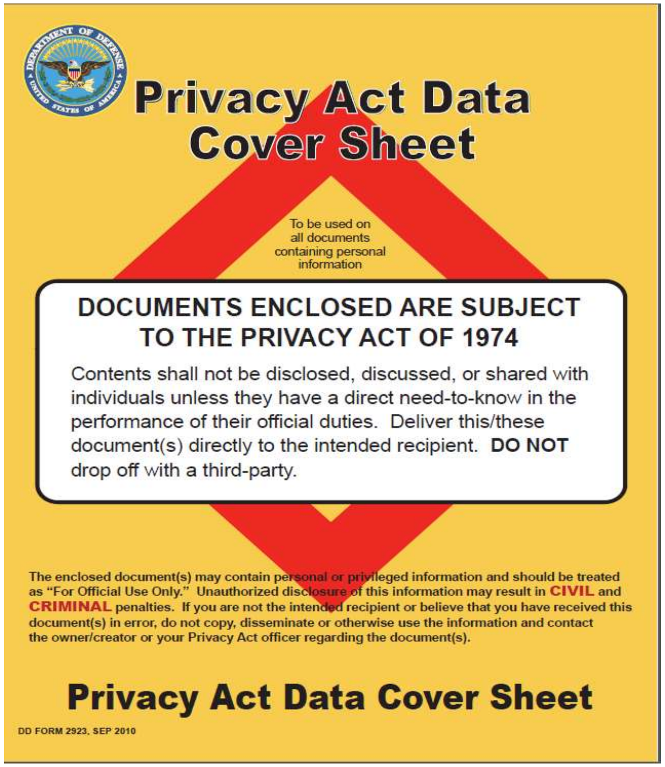
SF 902, CUI
Media Label



This medium is
CUI
U.S. Government Property

SF 903 (11-18)

SF 903, CUI Media
Label: USB size



Privacy Act Data
Cover Sheet

To be used on
all documents
containing personal
information

DOCUMENTS ENCLOSED ARE SUBJECT
TO THE PRIVACY ACT OF 1974

Contents shall not be disclosed, discussed, or shared with individuals unless they have a direct need-to-know in the performance of their official duties. Deliver this/these document(s) directly to the intended recipient. **DO NOT** drop off with a third-party.

The enclosed document(s) may contain personal or privileged information and should be treated as "For Official Use Only." Unauthorized disclosure of this information may result in **CIVIL** and **CRIMINAL** penalties. If you are not the intended recipient or believe that you have received this document(s) in error, do not copy, disseminate or otherwise use the information and contact the owner/creator or your Privacy Act officer regarding the document(s).

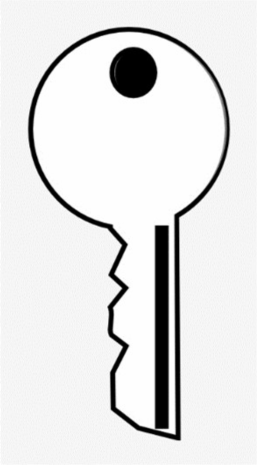
Privacy Act Data Cover Sheet

DD FORM 2923, SEP 2010

DD Form 2923
Cover Sheet

Storage of CUI

- During working hours - minimize the risk of access by unauthorized personnel through eavesdropping or observing CUI on:
  - Desks
  - Printers/faxes
  - Other publicly accessible areas, commute/travel status
- After working hours - if space provides security for continuous monitoring (i.e. Open Storage Areas), store in:
  - unlocked containers, desks, cabinets, etc.



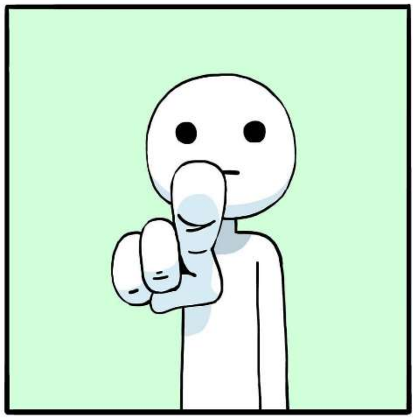
- For spaces without adequate monitoring, store in locked desks, file cabinets, bookcases, rooms, or similarly secured areas

Lawful Government Purpose

- Defined as any activity, mission, function, operation, or endeavor that the Government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement)

Similar to the concept of need-to-know for national security classified information

YOU, as the authorized holder of CUI, determine someone's lawful government purpose!



Destruction of CUI

- Any means approved for classified material
- NSA approved cross-cut shredders
- Locked gray shred bins

CUI must be:

- ✓ Unreadable
- ✓ Indecipherable
- ✓ Irrecoverable

- ➢ Do not destroy/shred CUI at home. Safeguard and bring back to NSWCCD
- ➢ Naval Nuclear Propulsion Information (NNPI) (classified or unclassified) must be destroyed in the same manner as classified information

Our Adversaries Are Relentless

NMCI - "U.S. Says Iran Hacked Navy Computers" – Wall Street Journal (2013)

U.S. Office of Personnel Management (OPM): 21.5 million affected (2015)

"Data Breach at Anthem May Forecast a Trend" – New York Times (2015)

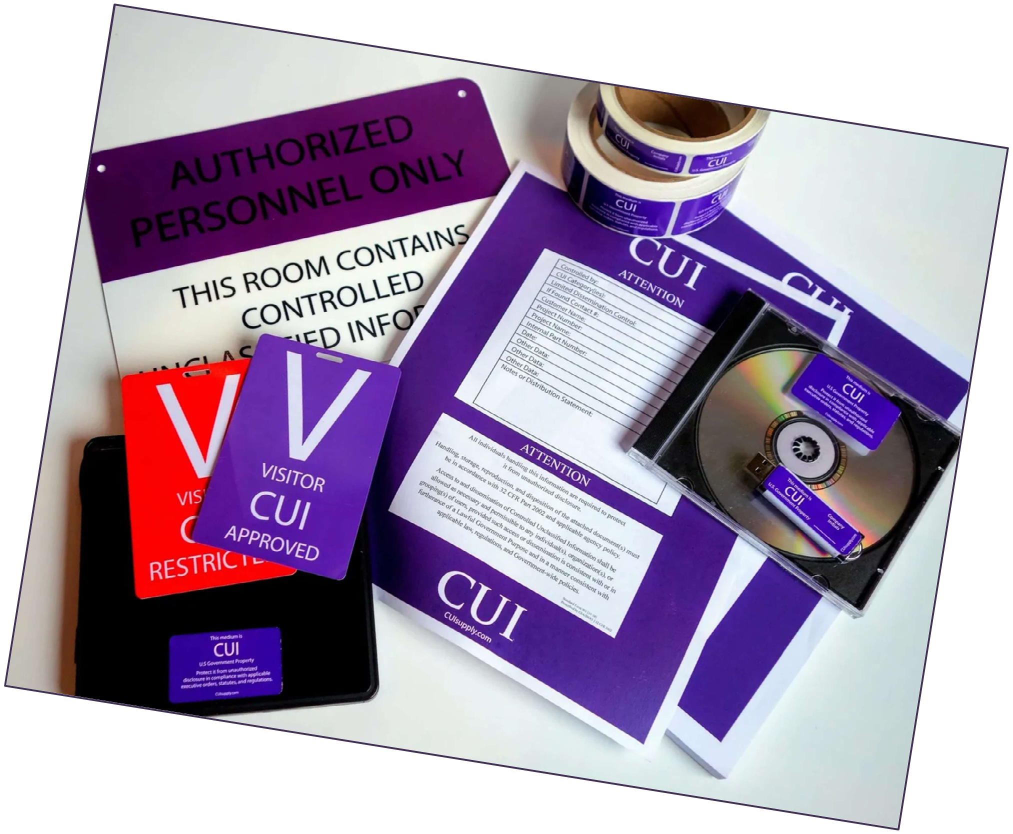
Microsoft: 250 million affected (2019)

"Twitter Confirms 'Nation-State' Attack: User Identities Breached" – Forbes (2020)

Zoom – A breach at the very beginning of the COVID-19 Pandemic (2020)

Questions?

QUESTIONS?
HOW?
WHERE?
WHEN?
WHO?
WHAT?
Where?
When?
Why?
What?


AUTHORIZED PERSONNEL ONLY
THIS ROOM CONTAINS CONTROLLED
V
VISITOR
CUI
APPROVED
RESTRICTED
CUI
ATTENTION
CUI
CUIsupply.com

Contact Information

Vicky Davis

Code 105 Security Office

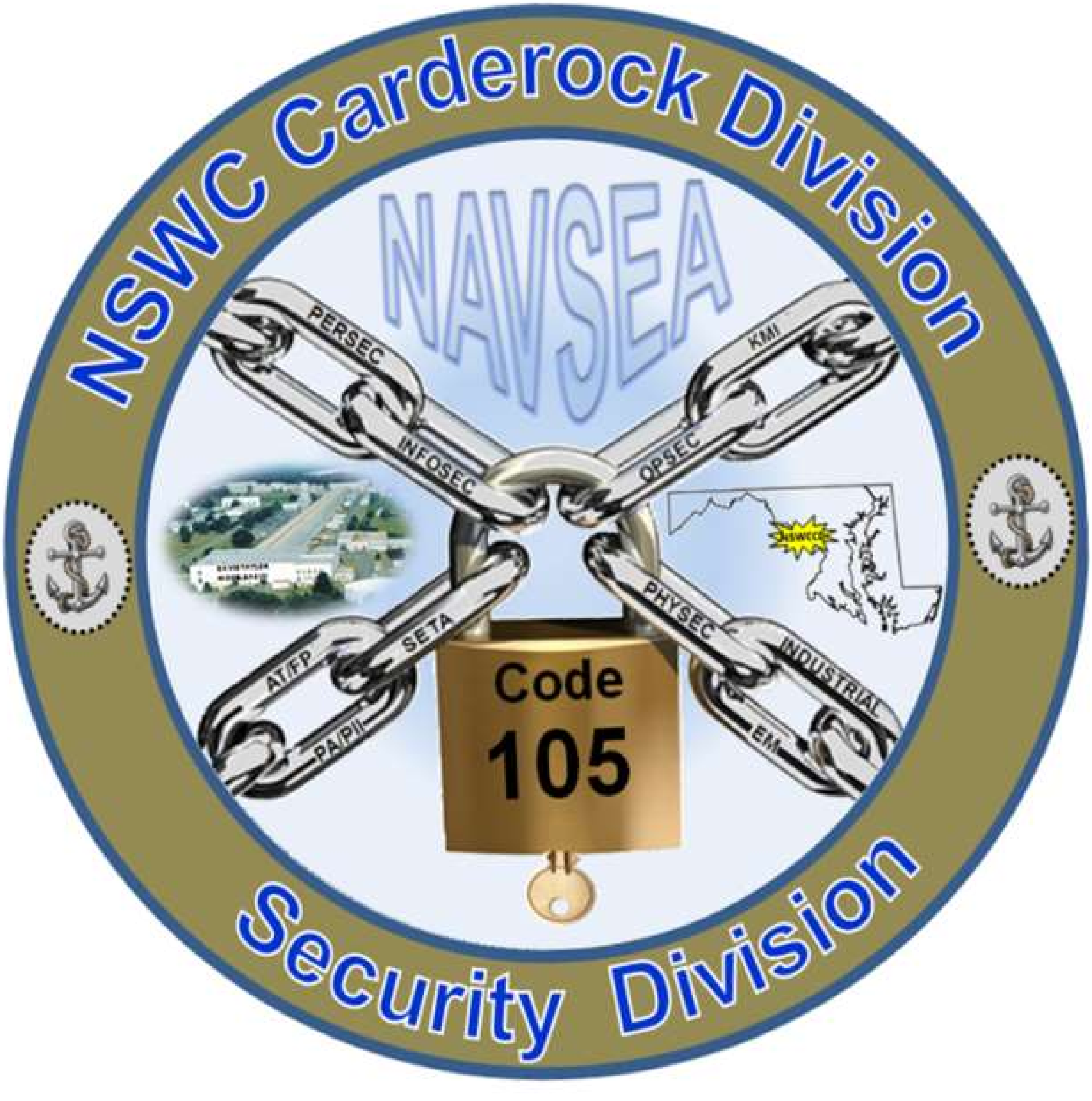
Building 42, Room 104

301-227-1408/5410

vicky.l.davis21.civ@us.navy.mil

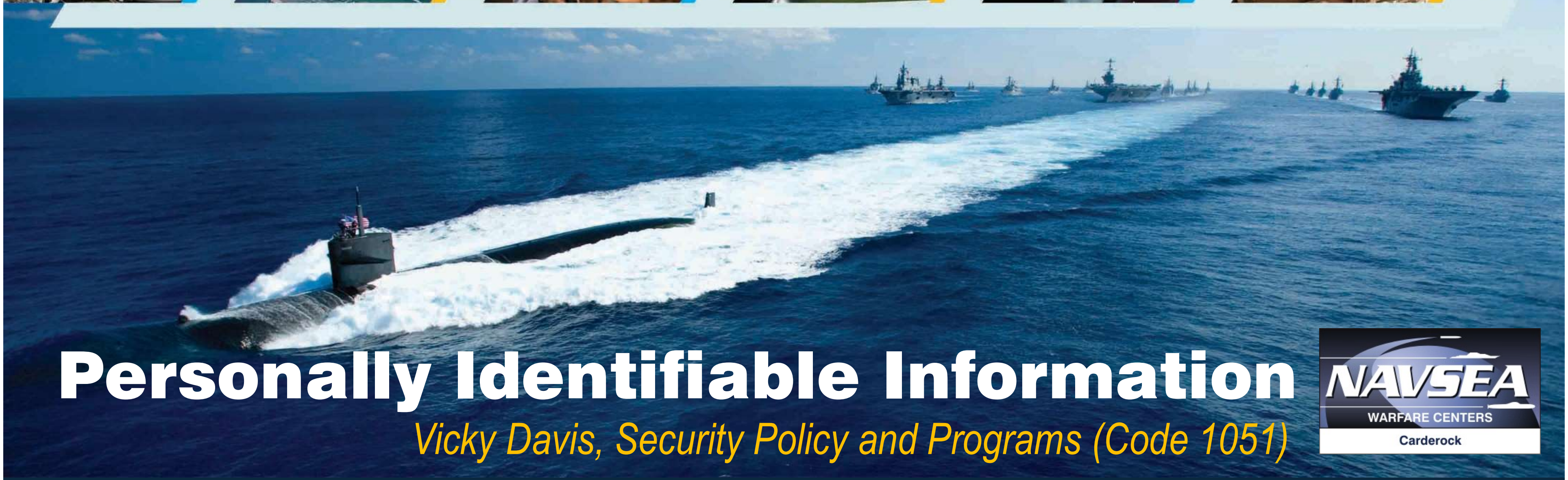
You, Me, Us, We

Security is a TEAM effort!


NSWC Carderock Division
NAVSEA
PERSEC
INFOSEC
KMI
OPSEC
NSWCCD
SETA
AT/FP
PA/PII
PHYSEC
INDUSTRIAL
EM
Code
105
Security Division

Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE



Personally Identifiable Information

Vicky Davis, Security Policy and Programs (Code 1051)

NAVSEA
WARFARE CENTERS
Carderock

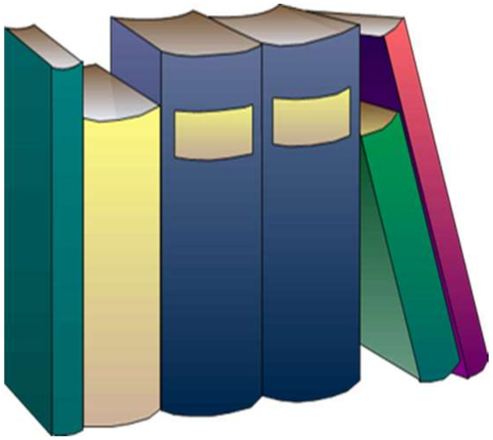
Captain Todd E. Hutchison
Commanding Officer, NSWCCD

Larry Tarasek
Technical Director, NSWCCD

Personally Identifiable Information (PII)

Defined as information about an individual that identifies, links, relates, or is unique to, or describes him or her, e.g., a SSN; age; rank; grade; marital status; race; salary; home/office phone numbers; other demographic, biometric, personnel, medical and financial information.

PII Policy/Resources



- DoD 5400.11-R, DOD Privacy Program
- SECNAVINST 5211.5F, DON Privacy Program
- NAVSEAINST 5211.2C, NAVSEA Privacy Act – PII Program
- CARDEROCKDIVINST 5211.1B, NSWCCD Privacy Program
- DODI 5200.48, Controlled Unclassified Information (CUI)
- NAVADMIN 125/10, Safeguarding Personally Identifiable Information
- DON MSG DTG 081745Z NOV 12, DON Fax Policy
- DON Chief Information Officer (CIO) website: http://www.doncio.navy.mil/Main.aspx

Helpful Links

- **Encrypting Email Containing PII:** http://www.doncio.navy.mil/ContentView.aspx?ID=3989
- **Rules for Handling PII by DON Contractor Support Personnel:** http://www.doncio.navy.mil/ContentView.aspx?ID=2145
- **PII and Records Management:** http://www.doncio.navy.mil/ContentView.aspx?ID=1415
- **Safeguarding PII on the Command Shared Drive:** http://www.doncio.navy.mil/contentview.aspx?id=755

"Go to" Guidance

Sensitive/Non-Sensitive PII

NAVSEA WARFARE CENTERS Carderock Division

"High risk" (Sensitive) PII: may cause harm to an individual if lost/compromised:

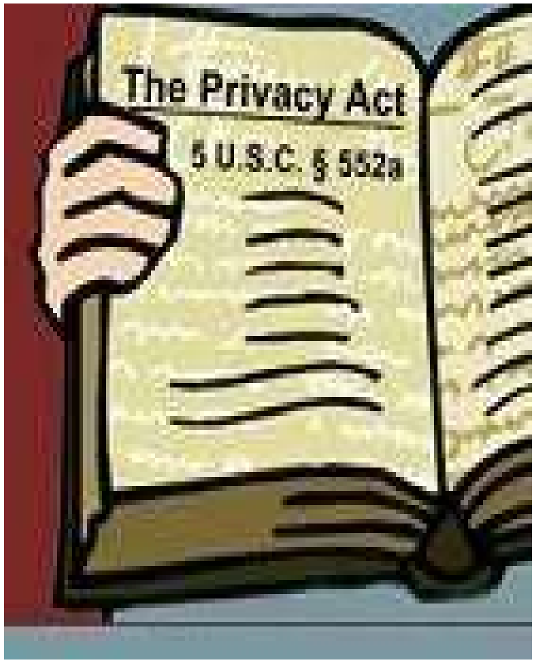
- Financial information - bank account #, credit card #, bank routing #
- Medical Data - diagnoses, treatment, medical history
- Full or truncated Social Security number
- Place and Date of Birth
- Mother's maiden name
- Passport #

"Low risk" (Non-sensitive) PII: business related PII; releasable under FOIA or authorized use under DON policy:

- Job Title
- Pay grade
- Office phone number
- Office address
- Office email address
- Full Name
- DoD ID/EDIPI
- DoD Benefits number

PII - Information about an individual that identifies, links, relates, or is unique to, or describes the individual which can be used to distinguish or trace an individual's identity.

Privacy Act of 1974



- Privacy Act OF 1974 - governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies.

- System of Records (SOR) - a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual, such as an SSN.

- No agency shall disclose any record that is contained in a SOR by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.

System of Records Notice (SORN)

- A public notice of all SOR under DoD control and retrievable by a personal identifier, e.g., name, SSN, date of birth, etc.

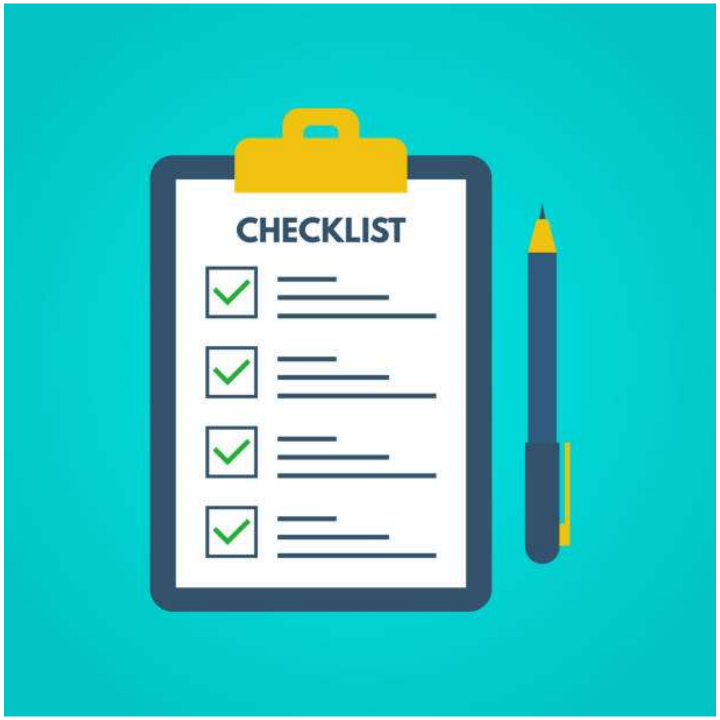
- Requirements:
  - Must list authority for soliciting Privacy Act (PA) information
  - Must be published by DoD in Federal Registry
  - Must include a ‘Routine Use’ Disclosure
  - Must be reviewed annually
  - Can’t be deleted, altered or amended
  - Must be posted to Defense Privacy and Civil Liberties Division web site at http://dpcld.defense.gov/ Privacy/SORNs/

Your Responsibilities

- ✓ Complete mandatory PII training via TWMS

- ✓ Apply the “lawful government purpose” principle (similar to need-to-know)

- ✓ Do not collect PII without an authorized SORN or maintain an unpublished SOR



- ✓ Obtain a reasonable verification of identity when a request to access PII is made

- ✓ Use DD 2923 and SF 901 Cover Sheets

- ✓ Report violations and/or misuse to your supervisor and PII Coordinator

Controlled Unclassified Information (CUI)

Personally Identifiable Information (PII) is a category of CUI

Apply “lawful government purpose” principle (similar to need-to-know)

Digitally sign and encrypt all emails containing CUI

Properly label and safeguard information

Add CUI banner markings to top/bottom of each page

Add Designation Indicator on right of first page/front cover

Use Cover Sheets:

DD 2923 for PII

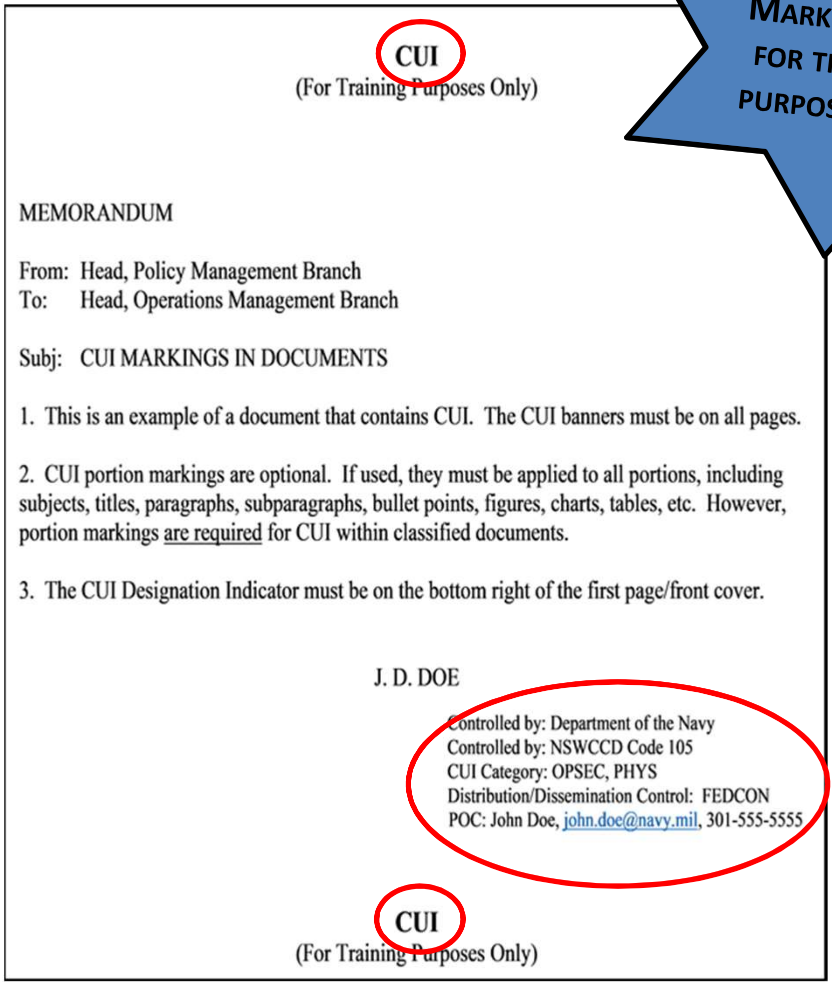
SF 901

Store CUI in locked desks, cabinets, etc. when not in use and not already in approved Open Storage Areas

Do not process or store CUI on personal computers/emails or post CUI on public websites/social media platforms

PII/CUI Marking Examples

MARKINGS ARE FOR TRAINING PURPOSES ONLY



CUI
(For Training Purposes Only)

MEMORANDUM

From: Head, Policy Management Branch
To: Head, Operations Management Branch

Subj: CUI MARKINGS IN DOCUMENTS

1. This is an example of a document that contains CUI. The CUI banners must be on all pages.

2. CUI portion markings are optional. If used, they must be applied to all portions, including subjects, titles, paragraphs, subparagraphs, bullet points, figures, charts, tables, etc. However, portion markings are required for CUI within classified documents.

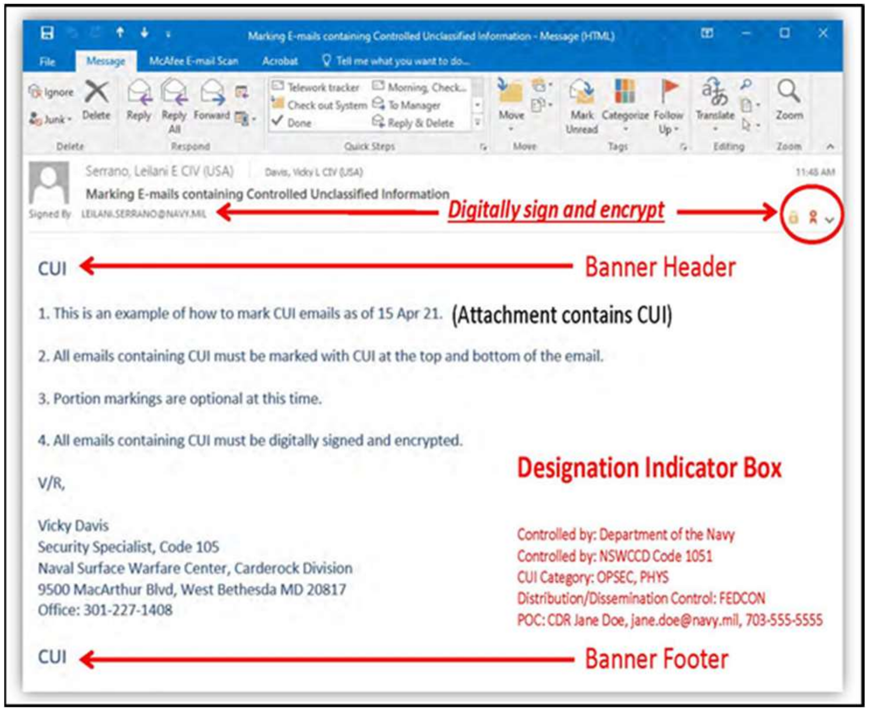
3. The CUI Designation Indicator must be on the bottom right of the first page/front cover.

J. D. DOE

Controlled by: Department of the Navy
Controlled by: NSWCCD Code 105
CUI Category: OPSEC, PHYS
Distribution/Dissemination Control: FEDCON
POC: John Doe, john.doe@navy.mil, 301-555-5555

CUI
(For Training Purposes Only)

- ✓ Banner markings top/bottom
- ✓ Designation Indicator on right



Serrano, Leilani E CIV (USA) | Davis, Vicky L CIV (USA) 11:48 AM
Marking E-mails containing Controlled Unclassified Information
Signed By LEILANI.SERRANO@NAVY.MIL

Digitally sign and encrypt

CUI ← Banner Header

1. This is an example of how to mark CUI emails as of 15 Apr 21. (Attachment contains CUI)

2. All emails containing CUI must be marked with CUI at the top and bottom of the email.

3. Portion markings are optional at this time.

4. All emails containing CUI must be digitally signed and encrypted.

V/R,

Vicky Davis
Security Specialist, Code 105
Naval Surface Warfare Center, Carderock Division
9500 MacArthur Blvd, West Bethesda MD 20817
Office: 301-227-1408

Designation Indicator Box

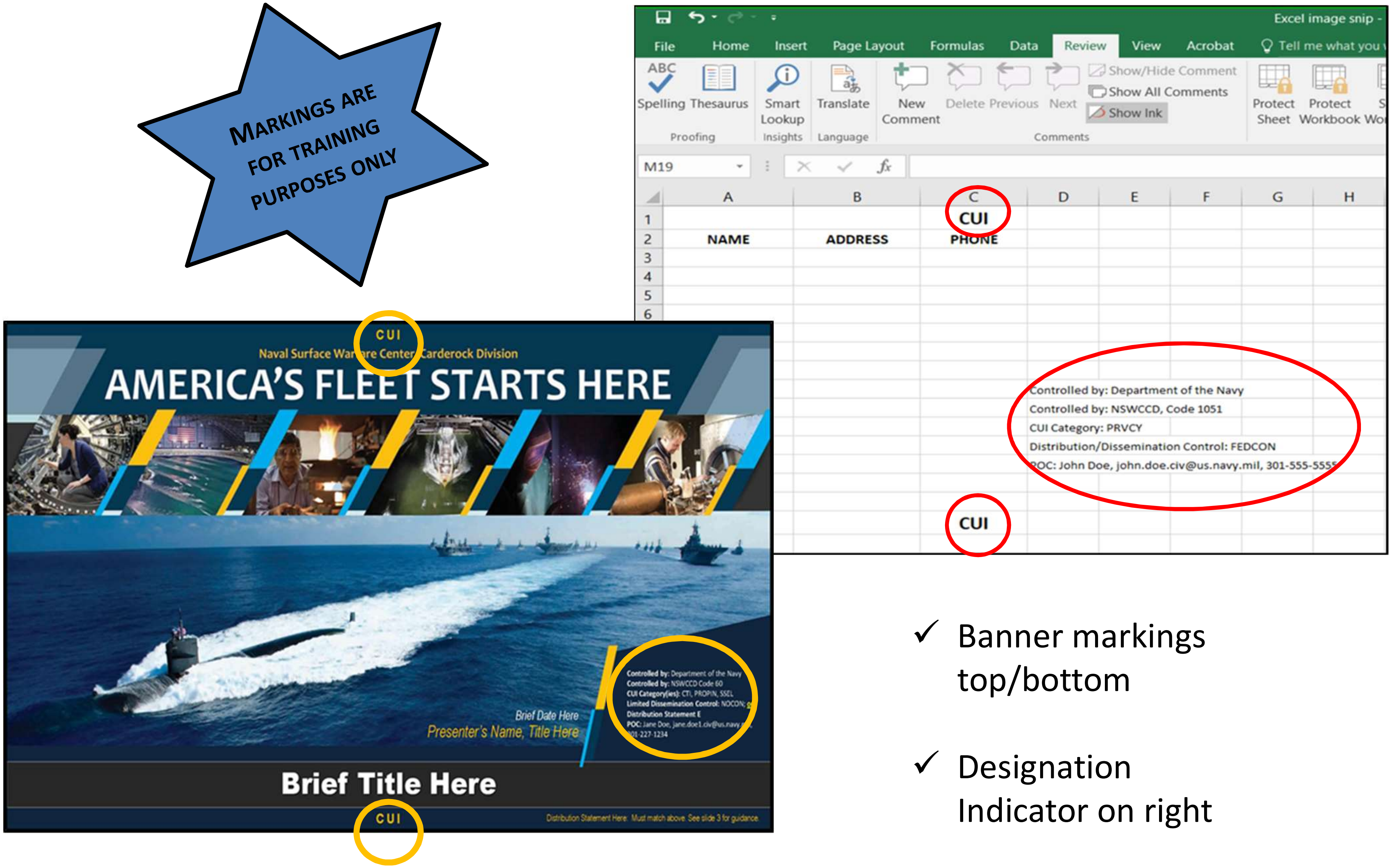
Controlled by: Department of the Navy
Controlled by: NSWCCD Code 1051
CUI Category: OPSEC, PHYS
Distribution/Dissemination Control: FEDCON
POC: CDR Jane Doe, jane.doe@navy.mil, 703-555-5555

CUI ← Banner Footer

PII/CUI Marking Examples

NAVSEA
WARFARE CENTERS
Carderock Division

MARKINGS ARE FOR TRAINING PURPOSES ONLY



CUI

NAME	ADDRESS	PHONE

Controlled by: Department of the Navy
Controlled by: NSWCCD, Code 1051
CUI Category: PRVCY
Distribution/Dissemination Control: FEDCON
POC: John Doe, john.doe.civ@us.navy.mil, 301-555-5555

CUI

CUI

Naval Surface Warfare Center Carderock Division

AMERICA'S FLEET STARTS HERE

Brief Date Here
Presenter's Name, Title Here

Controlled by: Department of the Navy
Controlled by: NSWCCD Code 60
CUI Category(ies): CTI, PROPIN, SSEL
Limited Dissemination Control: NOCON;
Distribution Statement E
POC: Jane Doe, jane.doe1.civ@us.navy.mil,
301-227-1234

Brief Title Here

CUI

Distribution Statement Here. Must match above. See slide 3 for guidance.

- ✓ Banner markings top/bottom
- ✓ Designation Indicator on right

Encrypt PII/CUI Emails!!

Digitally sign and encrypt emails containing PII/CUI

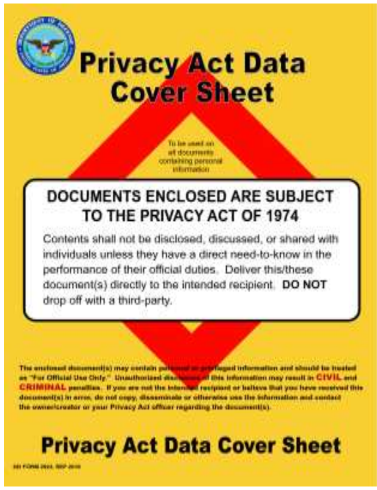
ALWAYS!!

PII Breach

Breach: Actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for an other than authorized purposes where one or more individuals will be adversely affected.

Breach Prevention:

- Complete annual mandatory PII training
- Follow Collections, Maintenance, and Use Policies
- Safeguard/Protect Information
  - ✓ Limit Access
  - ✓ Proper Transmittal (encrypt emails)
  - ✓ Use Coversheets
  - ✓ Proper Disposal
- Report violations and/or misuse to your supervisor and PII Coordinator



Privacy Act Data Cover Sheet

To be used on all documents containing personal information

DOCUMENTS ENCLOSED ARE SUBJECT TO THE PRIVACY ACT OF 1974

Contents shall not be disclosed, discussed, or shared with individuals unless they have a direct need-to-know in the performance of their official duties. Deliver this/these document(s) directly to the intended recipient. **DO NOT** drop off with a third-party.

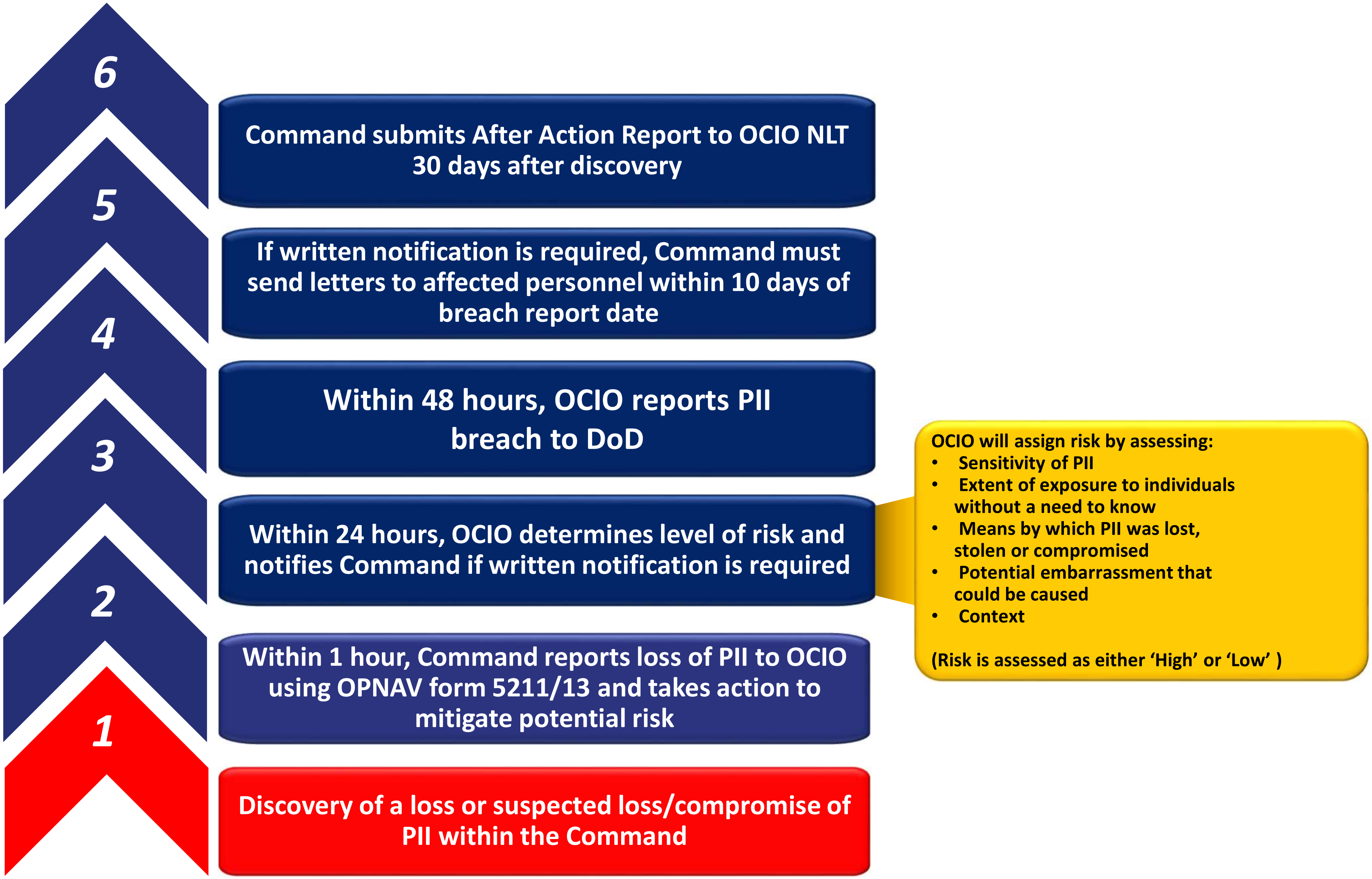
The enclosed document(s) may contain personal or privileged information and should be treated as "For Official Use Only." Unauthorized disclosure of this information may result in CIVIL and CRIMINAL penalties. If you are not the intended recipient or believe that you have received this document(s) in error, do not copy, disseminate or otherwise use the information and contact the owner/creator or your Privacy Act officer regarding the document(s).

Privacy Act Data Cover Sheet

DD FORM 2923, SEP 2010

DD Form 2923

DON PII Breach Reporting Process



6 Command submits After Action Report to OCIO NLT 30 days after discovery

5 If written notification is required, Command must send letters to affected personnel within 10 days of breach report date

4 Within 48 hours, OCIO reports PII breach to DoD

3 Within 24 hours, OCIO determines level of risk and notifies Command if written notification is required

2 Within 1 hour, Command reports loss of PII to OCIO using OPNAV form 5211/13 and takes action to mitigate potential risk

1 Discovery of a loss or suspected loss/compromise of PII within the Command

OCIO will assign risk by assessing:

- Sensitivity of PII
- Extent of exposure to individuals without a need to know
- Means by which PII was lost, stolen or compromised
- Potential embarrassment that could be caused
- Context

(Risk is assessed as either 'High' or 'Low')

Primary Cause....

NAVSEA WARFARE CENTERS Carderock Division

- Human error causes 80% of PII breaches
  - Not knowing guidance
  - Failure to follow established guidance
  - Carelessness

The most commonly reported PII breach - failure to encrypt emails
The most commonly breached PII element - SSNs

Faxes and PII

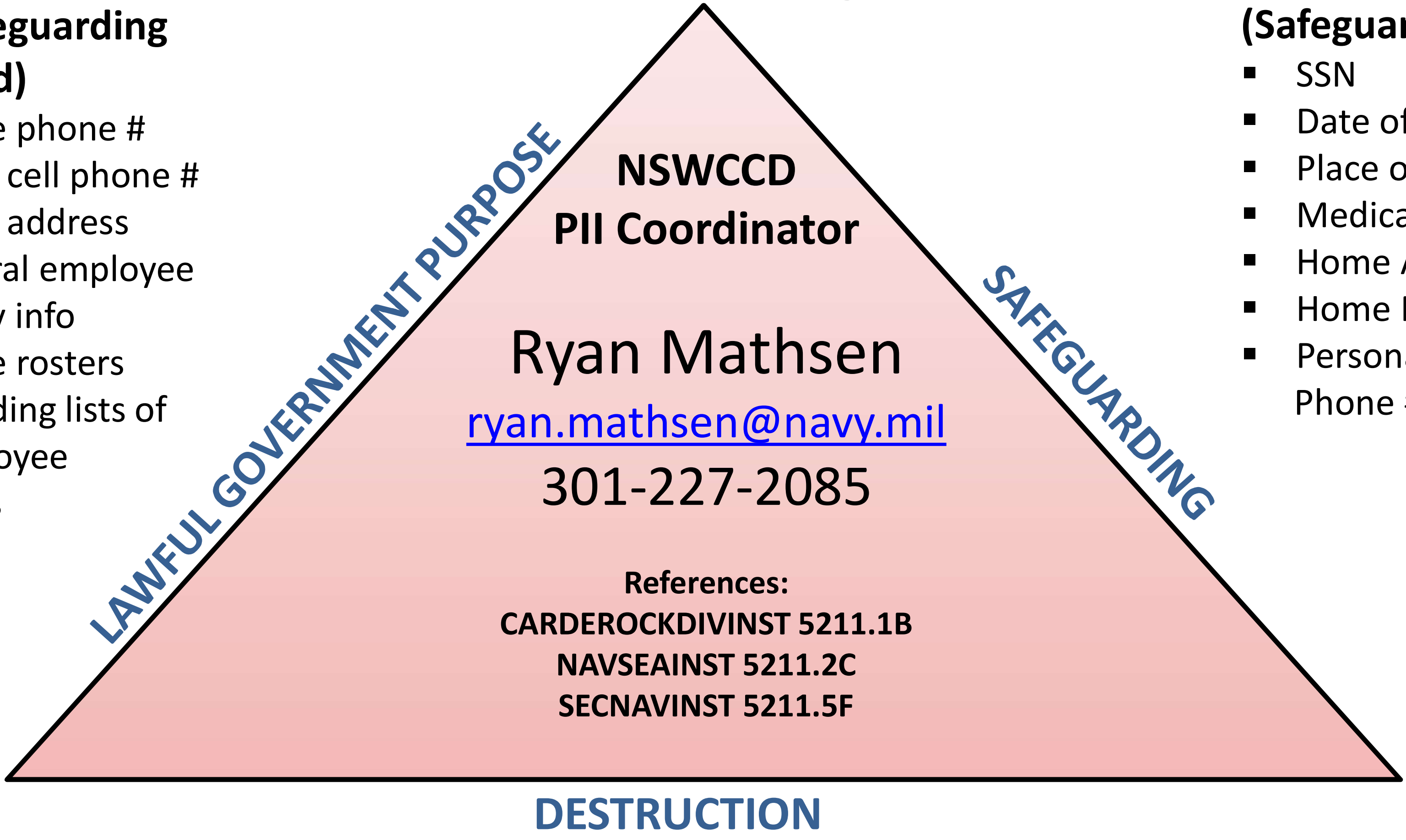
- **Faxing - one of the least secure means to transmit data**
  - ➢ Uses non-secure phone lines
  - ➢ Easy to send to wrong person/wrong FAX #
  - ➢ Copy of transmission often left on machine
  - ➢ Recipient may not immediately pick up document, exposing PII to others without a lawful government purpose

- **Alternative methods to faxing**
  - ➢ Send encrypted/digitally signed email
  - ➢ Use DOD Safe Access File Exchange (SAFE)
  - ➢ Use United States Postal Service snail mail

PII Triangle

Non-Sensitive PII (No safeguarding required)

- Office phone #
- Work cell phone #
- Work address
- Federal employee salary info
- Office rosters including lists of employee codes



LAWFUL GOVERNMENT PURPOSE

SAFEGUARDING

DESTRUCTION

NSWCCD
PII Coordinator

Ryan Mathsen
ryan.mathsen@navy.mil
301-227-2085

References:
CARDEROCKDIVINST 5211.1B
NAVSEAINST 5211.2C
SECNAVINST 5211.5F

Sensitive PII (Safeguard)

- SSN
- Date of Birth
- Place of Birth
- Medical Info
- Home Address
- Home Phone #
- Personal Cell Phone #

- **Lawful Government Purpose:** Does the person have a “lawful government purpose” (similar to need-to-know)? If not, do not forward or grant access.
- **Safeguarding:** * Encrypt ALL CUI/PII emails * Use DD 2923/SF 901 cover sheets * Mark CUI on all pages - headers/footers * Add Designation Indicator on first page/cover
- **Destruction:** Only destroy CUI/PII via NSA approved cross-cut shredders or locked gray shred bins. NEVER discard CUI/PII in a trash can, recycle bin, or dumpster.

Questions?

HOW?
WHERE?
Where?
WHEN?
WHERE?
WHO?
WHAT?
WHEN?
WHAT?
What?
WHERE?
WHAT?
WHERE?
HOW?
WHEN?
Where?
QUESTIONS?
What?
When?
When?
When?
WHERE?
Why?
WHEN?
When?
Where?
WHAT?
WHERE?
When?
When?
Why?
When?
WHO?
HOW?
WHAT?
Why?
When?
What?
HOW?
WHEN?
Why?
HOW?
What?

Contact Information

Vicky Davis

Code 105 Security Office

Building 42, Room 104

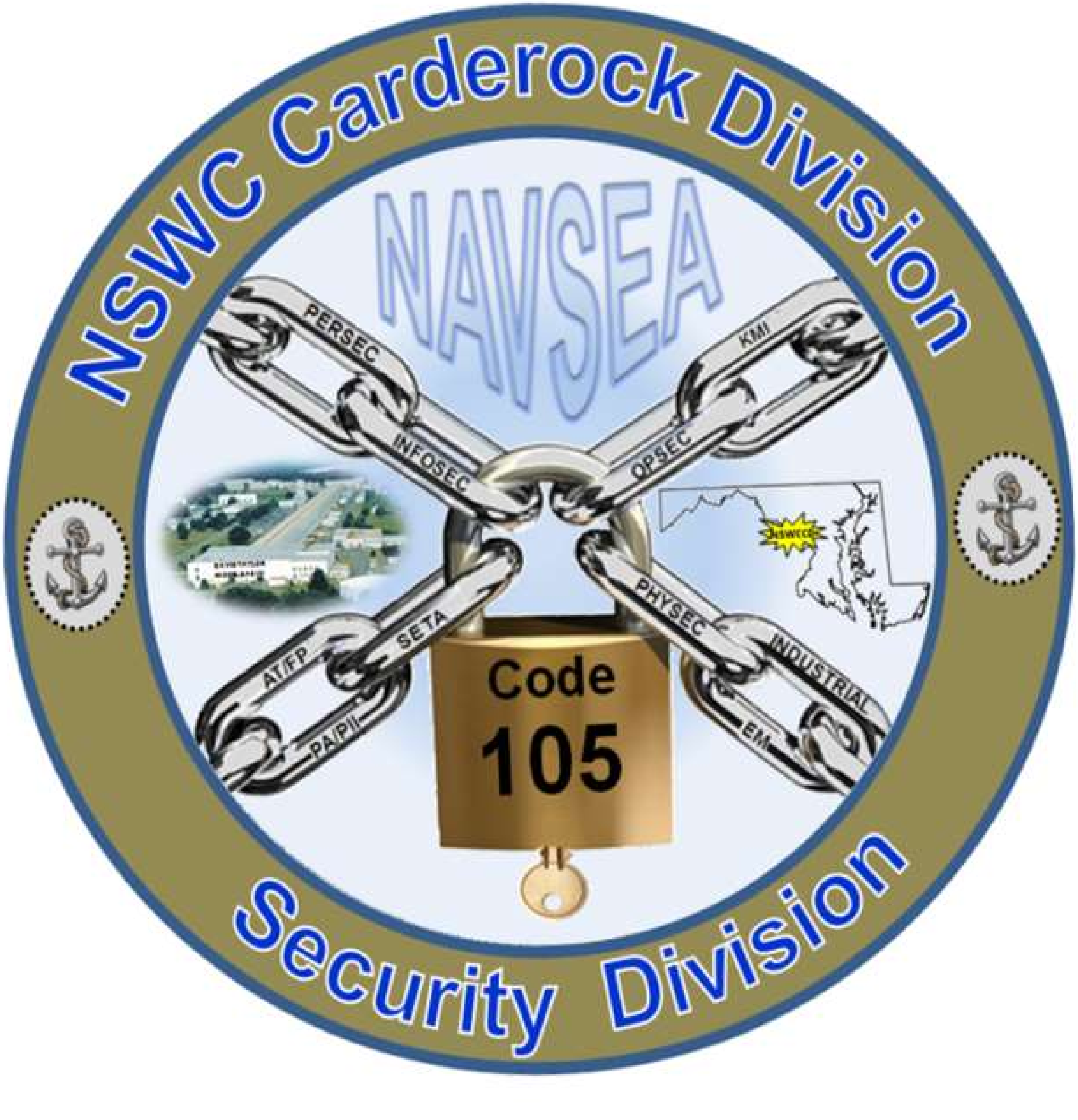
301-227-1408/5410

vicky.l.davis21.civ@us.navy.mil

You, Me, Us, We

Security is a

TEAM effort!

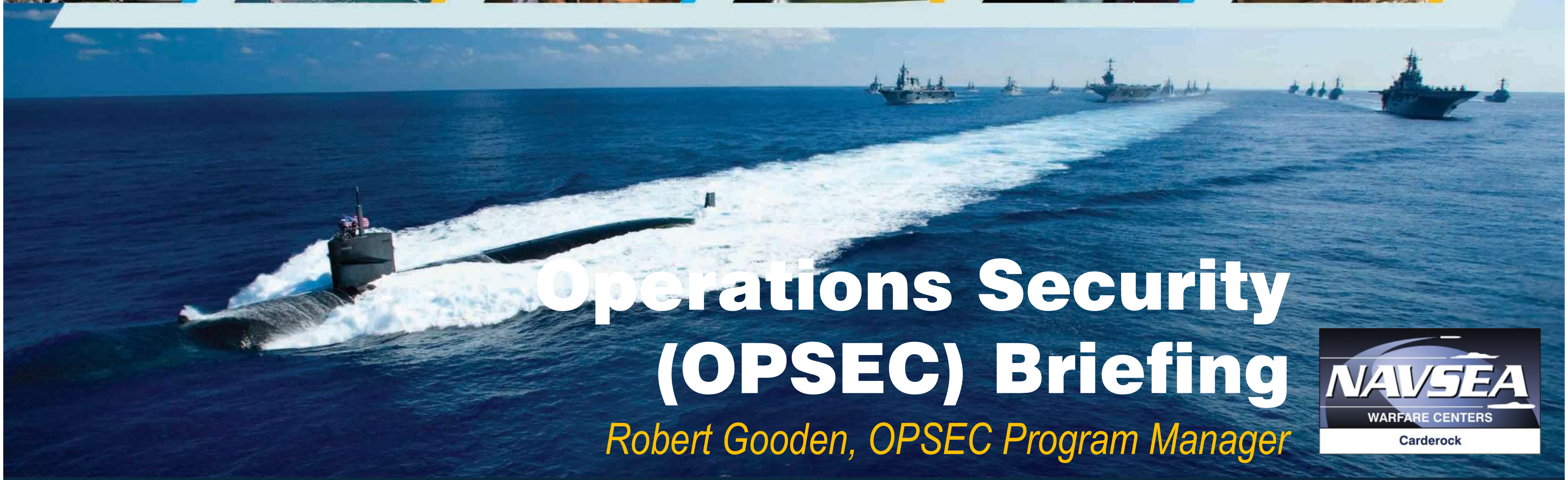

NSWC Carderock Division
NAVSEA
PERSEC
INFOSEC
KMI
OPSEC
NSWCCD
AT/FP
SETA
PA/PII
PHYSEC
INDUSTRIAL
EM
Code
105
Security Division

Break 2

Break 2

Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE



Operations Security (OPSEC) Briefing

Robert Gooden, OPSEC Program Manager

NAVSEA
WARFARE CENTERS
Carderock

Captain Todd E. Hutchison
Commanding Officer, NSWCCD

Larry Tarasek
Technical Director, NSWCCD

Overview

- History
- Definition & Perspective
- Oversight Guidance
- OPSEC & Traditional Security
- Five-Step Process
- OPSEC In-Depth
- OPSEC and the Internet
- TRASHINT
- OPSEC and Public Release
- Miscellaneous

History and Origins of OPSEC

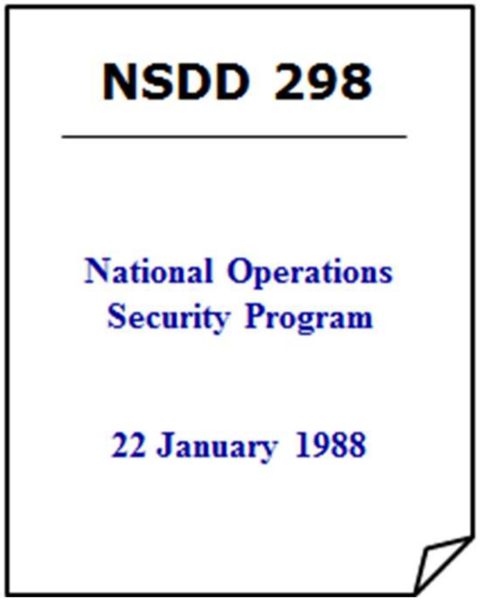
- Developed during the Vietnam War
- Study/analysis of how the enemy gained advance knowledge of combat air operations
- Established a methodology of looking at friendly ops from an adversary prospective
- The effort was code named – Purple Dragon
- Conceived processes to negate/reduce friendly indicators observable by the enemy
- Methodology was termed ‘Operations Security’
- National program formally established in 1988

The Purple Dragon

Presidential Authority

- National Security Decision Directive 298, “National Operations Security Program”

  Each Executive Department and Agency assigned or supporting national security missions with classified or sensitive activities shall establish a formal OPSEC program …



NSDD 298

National Operations
Security Program

22 January 1988

-- signed by President Ronald Reagan

OPSEC Defined

A systematic and proven process by which the U.S. Government and its supporting contractors can deny to potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive Government activities.

- National Security Decision Directive 298

DoD Directive 5205.02E

- “Applies to all activities that prepare, sustain, or employ U.S. Armed Forces during war, crisis, or peace.”
- “Including activities involving ***research, development, test and evaluation; DoD contracting; treaty verification; nonproliferation protocols; international agreements; force protection; and the release of information to the public***.”

Department of Defense
DIRECTIVE

[illegible]

DoD Operations Security (OPSEC) Program

20 June 2012

SECNAVINST 3070.2

- Establishes policy, procedures, and responsibilities for the Department of the Navy OPSEC program.
- The Secretariat, USN, and USMC shall maintain effective OPSEC programs that ensure coordination between public affairs, cybersecurity, security, operations, acquisition, intelligence, training , and command authorities and include mechanisms for enforcement , accountability, threat awareness, and oversight.
- OPSEC is to be incorporated into all operations and activities.

DEPARTMENT OF THE NAVY
[illegible]

[illegible]

[illegible]

OPERATIONS

SECURITY

5 May 2016

OPNAVINST 3432.1

- Directs Echelon II level commands (i.e., NAVSEA), possessing critical information, to establish formal OPSEC programs
- “Essential secrecy will be maintained by naval forces thru use of OPSEC measures……. OPSEC measures will be applied to research and system development, testing evaluation, and acquisition programs…..”
- Echelon II level commanders can delegate, to subordinate elements (Carderock), OPSEC program establishment requirements

[illegible]

OPERATIONS

SECURITY

4 August 2011

NAVSEAINST 3432.1A

- Directs establishment of OPSEC programs at designated NAVSEA field activities (i.e., Carderock). Delegates responsibility for NAVSEA OPSEC to the Director, Office of Security Programs and Planning
- Applies to all NAVSEA personnel (DoD civilians, military, and on-site contractors)
- “Establish and implement OPSEC policies, procedures, processes and guidance to enable the cost effective protection of NAVSEA critical information, people, technology, essential functions, and equipment.”

DEPARTMENT OF THE NAVY
[illegible]

NAVSEAINST 3432.1A
[illegible]

Naval Sea Systems
Command (NAVSEA)
Operations Security
(OPSEC) Policy

22 Nov 16

CARDEROCKDIVINST 3070.1

NAVSEA
WARFARE CENTERS
Carderock Division

- Directs division commander to establish a Carderock Division OPSEC program and designate a division OPSEC PM (delegated to Security Branch – 105)
- Applies to all departments and offices of Carderock Division
- Supplements OPSEC concepts, policies, and procedures of DON and NAVSEA

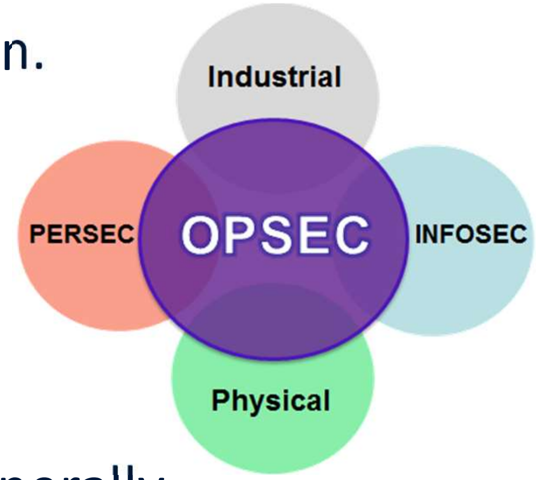
DEPARTMENT OF THE NAVY
[illegible]

Naval Surface Warfare Center - Carderock Division Operations Security (OPSEC) Program

1 Oct 2015

Relationship to Traditional Security

- Security programs protect ***CLASSIFIED*** information.
  - Personnel Security
  - INFOSEC
  - Industrial Security
  - Physical Security



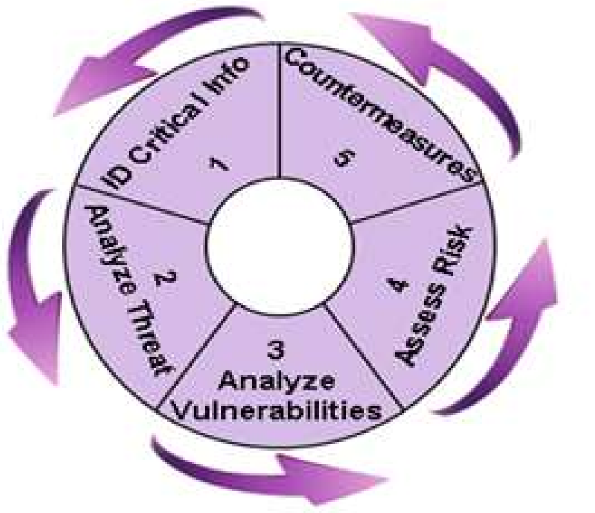
- OPSEC measures identify, control, and protect generally ***UNCLASSIFIED*** (critical) information associated with sensitive operations and activities.

- OPSEC is a ***COUNTERMEASURES*** program.

OPSEC does not replace traditional security disciplines —
it STRENGTHENS them.

OPSEC 5-Step Process

- Identify Critical Information
- Analyze the Threat
- Determine Vulnerabilities
- Risk Assessment
- Develop / Apply Countermeasures



'A Continuous Process'

OPSEC's most important characteristic is that it is a process that can be applied to any operation or activity.

What is Critical Information?

- Specific facts about friendly intentions, capabilities, and activities

- Probably unclassified, but still sensitive

- Two or three bits of critical information aggregated together may result in a sensitive disclosure

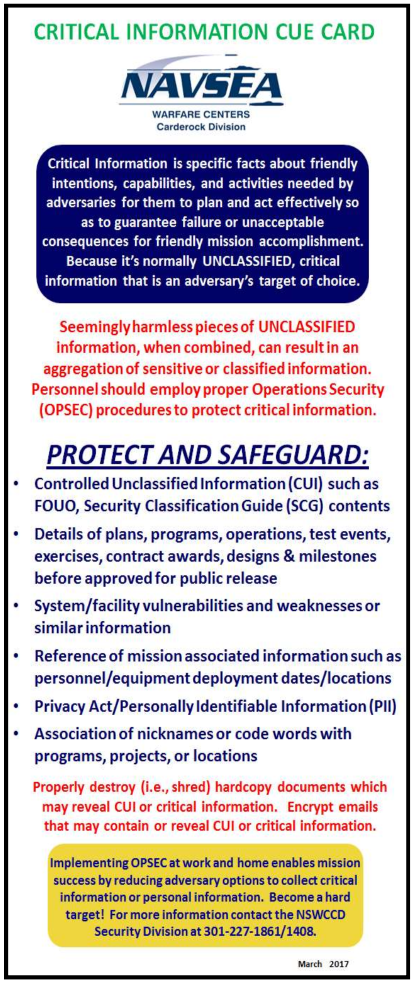
Data aggregation becomes the puzzle pieces revealing the 'big picture'

The information that is often used against us is not classified; it is information that is openly available to anyone who knows where to look and what to ask.

Critical Information

NAVSEA WARFARE CENTERS Carderock Division

- Command Critical Information List (CIL) and Code specific CIL are posted on intranet
- CO's OPSEC Policy Memo stresses importance of protecting critical information
- Review CIL Cue Cards posted at all desks/workstations



CRITICAL INFORMATION CUE CARD

NAVSEA WARFARE CENTERS Carderock Division

Critical Information is specific facts about friendly intentions, capabilities, and activities needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. Because it's normally UNCLASSIFIED, critical information that is an adversary's target of choice.

Seemingly harmless pieces of UNCLASSIFIED information, when combined, can result in an aggregation of sensitive or classified information. Personnel should employ proper Operations Security (OPSEC) procedures to protect critical information.

PROTECT AND SAFEGUARD:

- Controlled Unclassified Information (CUI) such as FOUO, Security Classification Guide (SCG) contents
- Details of plans, programs, operations, test events, exercises, contract awards, designs & milestones before approved for public release
- System/facility vulnerabilities and weaknesses or similar information
- Reference of mission associated information such as personnel/equipment deployment dates/locations
- Privacy Act/Personally Identifiable Information (PII)
- Association of nicknames or code words with programs, projects, or locations

Properly destroy (i.e., shred) hardcopy documents which may reveal CUI or critical information. Encrypt emails that may contain or reveal CUI or critical information.

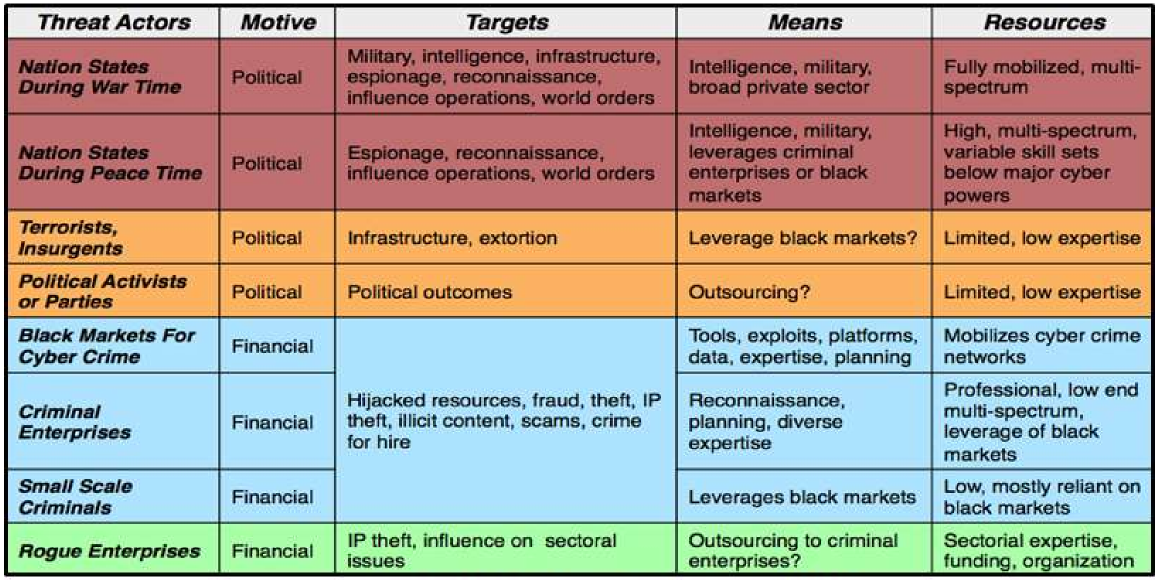
Implementing OPSEC at work and home enables mission success by reducing adversary options to collect critical information or personal information. Become a hard target! For more information contact the NSWCCD Security Division at 301-227-1861/1408.

March 2017

Analyze the Threat

"The capability of an adversary coupled with the intention to undertake any actions detrimental to the success of program activities or operations."

- – Nation states
- – Insiders
- – Criminal elements
- – Terrorists
- – Narcotics traffickers



Threat Actors	*Motive*	*Targets*	*Means*	*Resources*
Nation States During War Time	Political	Military, intelligence, infrastructure, espionage, reconnaissance, influence operations, world orders	Intelligence, military, broad private sector	Fully mobilized, multi-spectrum
Nation States During Peace Time	Political	Espionage, reconnaissance, influence operations, world orders	Intelligence, military, leverages criminal enterprises or black markets	High, multi-spectrum, variable skill sets below major cyber powers
Terrorists, Insurgents	Political	Infrastructure, extortion	Leverage black markets?	Limited, low expertise
Political Activists or Parties	Political	Political outcomes	Outsourcing?	Limited, low expertise
Black Markets For Cyber Crime	Financial	Hijacked resources, fraud, theft, IP theft, illicit content, scams, crime for hire	Tools, exploits, platforms, data, expertise, planning	Mobilizes cyber crime networks
Criminal Enterprises	Financial		Reconnaissance, planning, diverse expertise	Professional, low end multi-spectrum, leverage of black markets
Small Scale Criminals	Financial		Leverages black markets	Low, mostly reliant on black markets
Rogue Enterprises	Financial	IP theft, influence on sectoral issues	Outsourcing to criminal enterprises?	Sectorial expertise, funding, organization

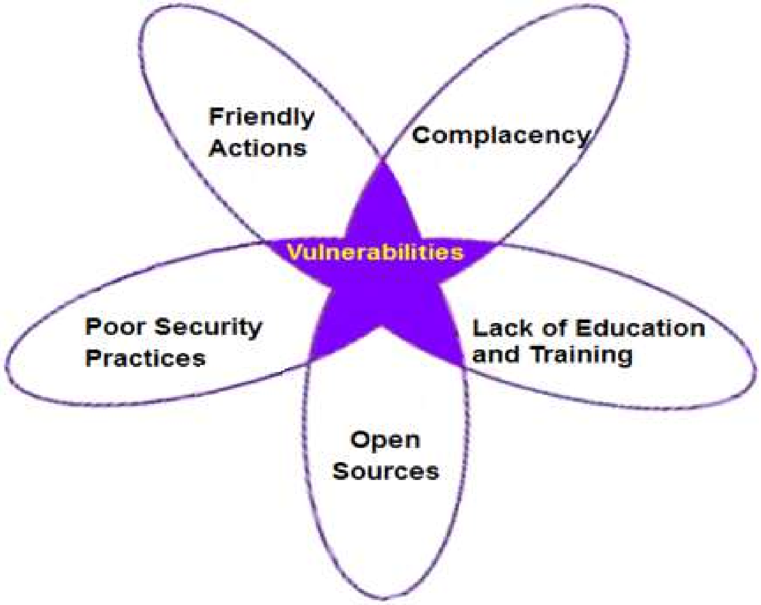
Threat Actors and Capabilities

Threat = Capability + Intent

Vulnerabilities

'Weaknesses which are susceptible to exploitation by adversaries. A vulnerability exists when the adversary is capable of collecting an OPSEC indicator, correctly analyzing it, and then taking timely action.'

- Observation of friendly actions
- Open source research
- Poor security processes
- Lack of education and training
- Complacency / predictability



Vulnerability + Threat = Risk

Indicators

'Friendly actions and open sources of information that can be detected or interpreted by adversarial intelligence systems.'

- Signatures – make indicators identifiable and stand out
- Associations – relationships to other information or activities
- Profiles - sum of multiple signatures (patterns)
- Contrasts - established pattern vs. current observations
- Exposure – duration and time an indicator can be observed

Allows the adversary to identify our critical information

Risk Assessment

- Risk management, not risk avoidance

- **Threat** + No Vulnerability = No Risk
- No Threat + **Vulnerability** = No Risk
- ***Threat + Vulnerability = Risk***

- Justify the cost of losing information vs. the cost of implementing countermeasures

Risk is the likelihood of an undesirable event occurring
and the consequences of that event.

Apply Countermeasures

- Prevent detection of critical information
- Provide an alternative association of critical information
- Deny the adversary’s collection system
- Implement new, more stringent procedural actions

$$$ - Cost is the biggest factor in implementing specific countermeasures

Basic Countermeasures

- All Paper, Notes, Printouts etc.– **NAVSEA Shred Policy**
- Sensitive/classified e-mails – **Encryption or use SIPRNET**
- Phone Calls **– STE**
- Sensitive/classified info documents – **SIPR/Secure Fax**
- DO NOT **"TALK AROUND"** Sensitive Information on Non-Secure Voice Circuits
- No **"Pillow Talk"** (guard what's shared with significant others)
- No **"Shop Talk"** in restaurants, bars, public areas

The best countermeasure is to adhere to established security procedures

OPSEC and the Internet

- Recovered al Qaida training manual states:
  - “Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy”
- DoD Website Admin Policy - review data for sensitivity before posting to publicly accessible websites (www.defenselink.mil/webmasters)
- OPSEC policy requirement to conduct periodic web site reviews/research for presence of sensitive information

Policy requirement for OPSEC PMs to conduct periodic web site reviews/research for presence of sensitive information

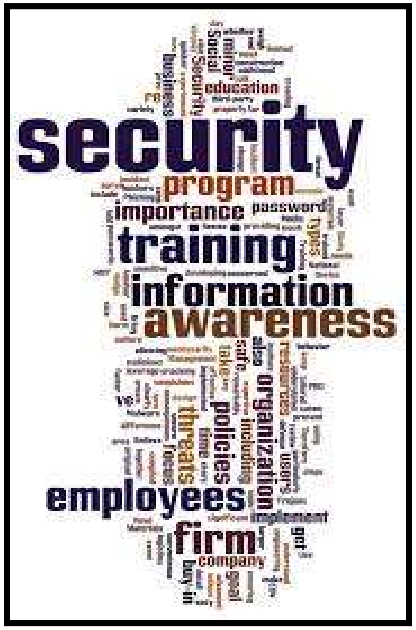
Social Networking Sites

- Current problem
- Adhere to SECDEF DoD policy
- Jun 2009 Deputy Director Memo
- Absolutely no expectation of privacy
- Pose a **significant** OPSEC, intelligence, and general security **threat to DON personnel, facilities, and mission**

DON employees are prohibited from posting information about DON personnel, missions, activities, and operations unless it is readily available to the general public AND has been authorized of public release IAW DoD guidance

OPSEC and Official IT Networks

- Technical nature of system passwords warrant added protections
- Don’t share passwords with co-workers or unauthorized users
- Risks are information compromise/system degradation
- Sys Admins: Transmit router settings and passwords separately and always encrypt

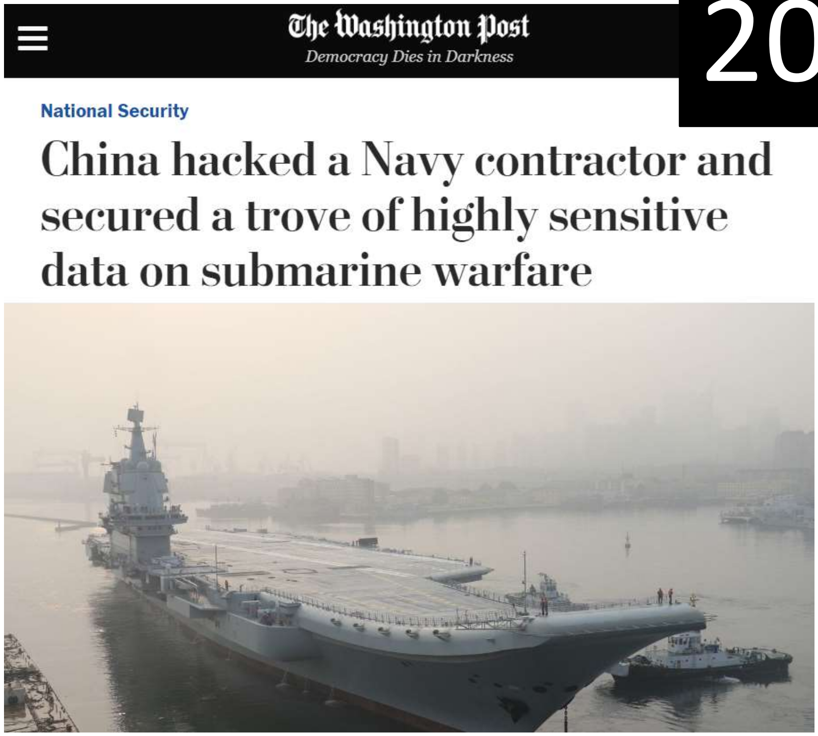


CTF 1010 MSG, DTG 120537Z AUG 17, Subj: OPSEC Handling of Network Settings and Passwords

Our Adversaries Are Relentless

“Australian defense firm was hacked and F-35 data stolen, DoD confirms” – arstechnica.com, 2017

2018

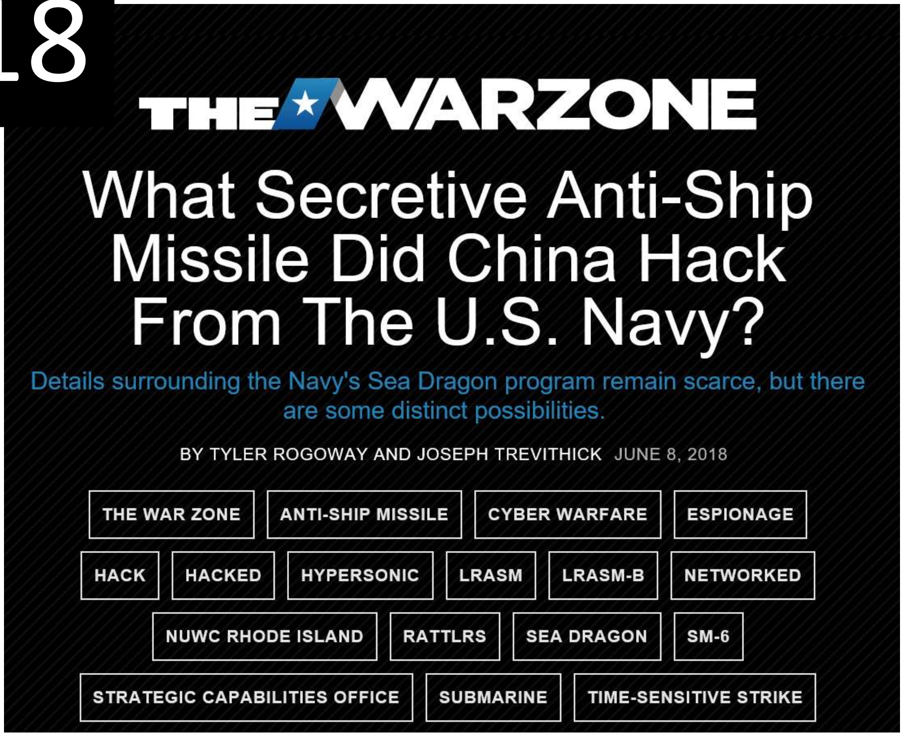


The Washington Post

Democracy Dies in Darkness

National Security

China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare



THE WARZONE

What Secretive Anti-Ship Missile Did China Hack From The U.S. Navy?

Details surrounding the Navy's Sea Dragon program remain scarce, but there are some distinct possibilities.

BY TYLER ROGOWAY AND JOSEPH TREVITHICK JUNE 8, 2018

THE WAR ZONE | ANTI-SHIP MISSILE | CYBER WARFARE | ESPIONAGE | HACK | HACKED | HYPERSONIC | LRASM | LRASM-B | NETWORKED | NUWC RHODE ISLAND | RATTLRS | SEA DRAGON | SM-6 | STRATEGIC CAPABILITIES OFFICE | SUBMARINE | TIME-SENSITIVE STRIKE

TRASHINT

Dumpster-dives of random refuse collection points

<u>Examples of Critical Information Found</u>

Personally Identifiable Info (PII)

Official e-mails

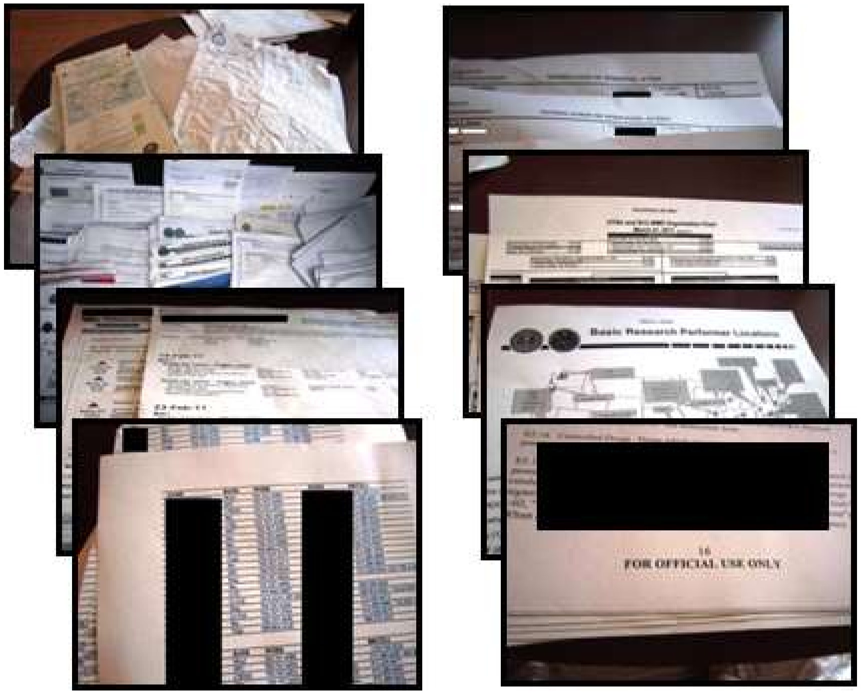
Funding/resource/budget information

Office Memos

FOUO

Personal banking account numbers

Technical briefings



TRASHINT Countermeasures

- Periodically inspect outgoing trash and recycle containers
- Utilize approved shredders and burn bags
- Securely store sensitive information pending destruction

OPSEC and Public Release

- Official news articles
- Briefing presentations
- Training/informational brochures, pamphlets, etc.
- Manuscripts for books/movies/plays (fiction or non-fiction)
- Personal (unofficial) blogs
- SNS forums
- Ensure applicable time allowance (edits/conflicts)
- Restrictive/Limited Distribution Statements (A-F)

Pre-publication review is mandatory IAW DoDI 5230.29; DEPSECDEF & CJCS Jnt Msg DTG 090426Z AUG 06; DoDI 8550.01; and DoD 5205.02-M. Additionally, SF-312, Nondisclosure Agreement.

OPSEC: Capture The Flag

OPSEC: Capture The Flag

Your Responsibilities

- Ask Yourself --
  - ✓ Is this information important to our adversaries?
  - ✓ Do I care if it is **published on the front page** of the Washington Post?
  - ✓ Will it help an adversary to assemble and form the **overall picture**?
  - ✓ Is this information central to the mission effectiveness of NSWCCD or my office?
  - ✓ What might this "insignificant" information reveal to adversaries about our **intentions** and **capabilities**?

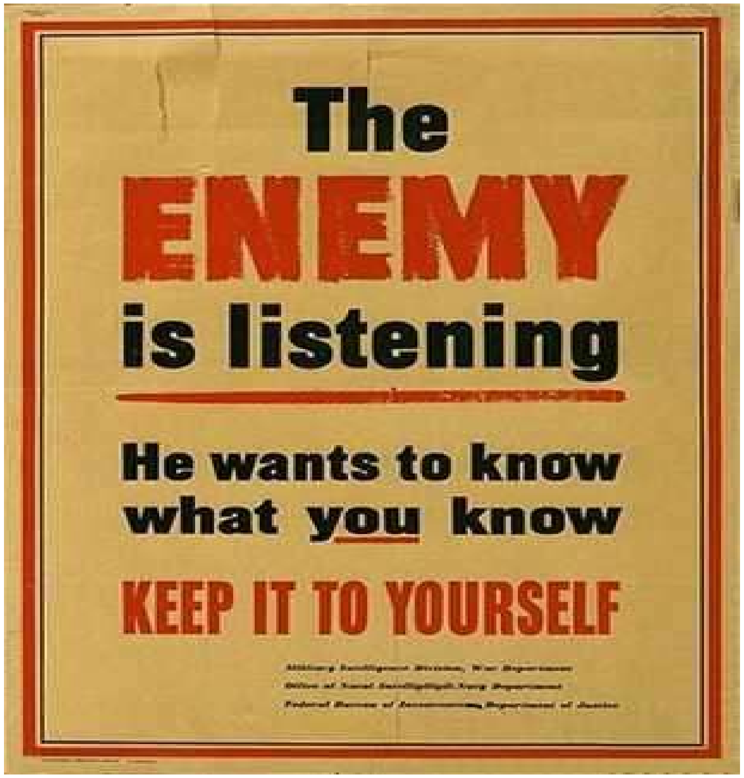
- What will our adversaries learn by watching, listening, and collecting information we "protect?"

OPSEC Summary

- ***Identify critical information*** to determine if friendly actions can be observed by adversary intelligence systems.
- ***Determine if information*** obtained by adversaries ***could be interpreted*** to be useful to them.
- ***Execute*** selected ***countermeasures*** that eliminate or reduce adversary exploitation of friendly critical information.

OPSEC helps identify the indicators that give away information about missions, activities and operations.

Still Important Today



The

ENEMY

is listening

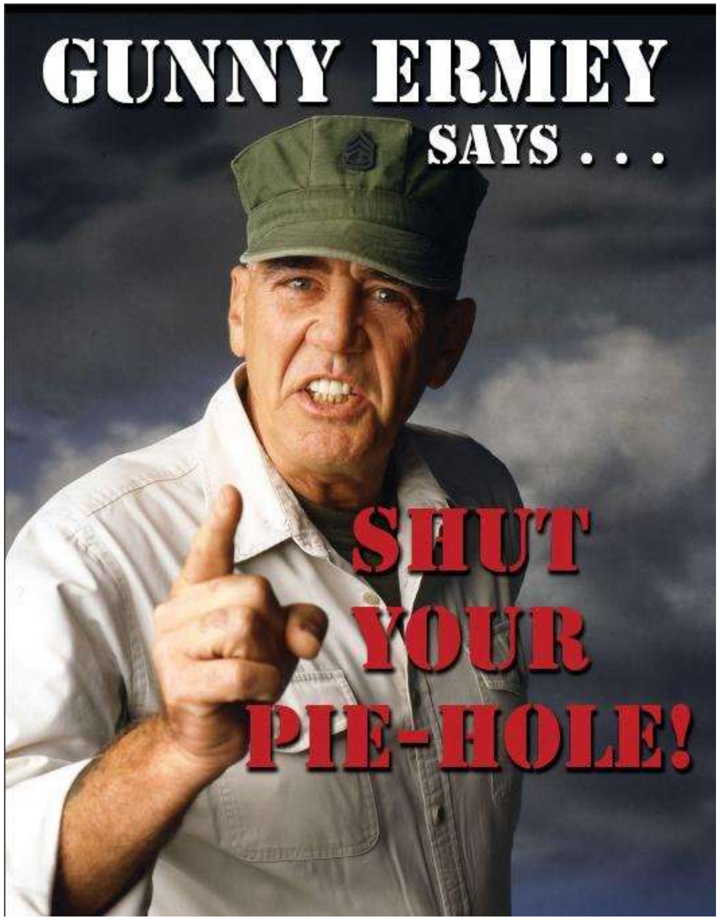
He wants to know what you know

KEEP IT TO YOURSELF

Military Intelligence Division, War Department
Office of Naval Intelligence, Navy Department
Federal Bureau of Investigation, Department of Justice

World War II Era Poster

Still Important Today



Modern Era Poster

Contact Information

Cliff Young
Security Division (Code 105)
Building 42, Room 104
301-227-1861
Clifford.young@navy.mil

Remember…Think OPSEC!!

Security is Everyone's Responsibility – If You See Something, Say Something!

NSWC Carderock
NAVSEA
PERSONNEL
INFOSEC
COMSEC
OPSEC
DAVID TAYLOR MODEL BASIN
NSWCCD
SETA
AT/FP
PHYSICAL
INDUSTRIAL
Code
105
Security Division

Naval Surface Warfare Center, Carderock Division

AMERICA'S FLEET STARTS HERE

NAVSEA
WARFARE CENTERS
Carderock

FY22 Insider Threat Awareness Training

Security Division (Code 105)

UNCLASSIFIED

Insert appropriate Distribution or CUI statement here

Captain Todd E. Hutchison
Commanding Officer, NSWCCD

Larry Tarasek
Technical Director, NSWCCD

Insider Threat POCs

Rachael Bass (Program Manager)
rachael.t.bass.civ@us.navy.mil

Terry Tate (Alternate)
terry.l.tate.civ@us.navy.mil

Brandon Reilly (Branch Chief)
brandon.r.reilly.civ@us.navy.mil

For general security information and inquiries call: 301-227-1408

Insert appropriate Distribution or CUI statement here

Insider Threat Agenda

NAVSEA WARFARE CENTERS Carderock Division

- Security Message
- Basic Insider Threat Definitions
- Significance of Insider Threat
- Fighting the Insider Threat
- Recognizing the Insider Threat
- Reporting the Insider Threat
- Case Studies
- Summary

Insert appropriate Distribution or CUI statement here

Security Message

The protection of U.S. Government assets including people, property, and both classified and controlled unclassified information is the responsibility of each and every member of the Department of Navy (DON), regardless of how it was obtained or what form it takes. Anyone with access to these resources has an obligation to protect it; a simply “I didn’t know” just won’t cut it.

The very nature of our jobs dictates we must lead the way in sound security practices. This Insider Threat training provides an overview for security education, training, and awareness.

Our vigilance is imperative!

Basic Insider Threat Definitions

Insider threat **-** a person with authorized access, who uses that access wittingly or unwittingly to harm national security interests through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in loss of degradation of resources or capabilities. The term kinetic can include, but is not limited to, “the threat of harm from sabotage or workplace violence.”

Insider **-** Any person with authorized access to DoD resources by virtue of employment, volunteer activities, or contractual relationship with DoD.

Threat **-** A person having the intent, capability, and opportunity to cause loss or damage.

Access **-**The ability and opportunity to obtain knowledge of classified sensitive information or to be in a place where one could expect to gain such knowledge**.**

Asset **-** Person, structure, facility, information, material, or process that has value**.**

Classified Information **-** Official information that has been determined to require, in the interests of national security, protection against unauthorized.

Basic Insider Threat Definitions (continued)

Cleared Contractor (CC) - A person or facility operating under the National Industrial Security Program (NISP) that has had an administrative determination that they are eligible, from a security point of view, for access to classified information of a certain level.

Controlled Unclassified Information - Unclassified information that does not meet the standards for National Security Classification under EO 12958 but is (1) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (2) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

Disgruntled Employee - An employee who may be annoyed, discontent, displeased, dissatisfied, grumpy, irritated, malcontent, or upset to the point that he may take violent action against a coworker, supervisor, or employer.

Personal Identifiable Information (PII) - Information that can be used to distinguish or trace an individual's identity. This includes: names; social security number; date and place of birth; rank/paygrade, phone number and biometric records or any other personal information that is linked or linkable to a specified individual.

Risk - a measure of consequence of peril, hazard, or loss, which is incurred from a capable aggressor or the environment (the presence of a threat and unmitigated vulnerability).

Why is the Insider Threat Significant

An insider threat can have a negative impact on national security and industry resulting in:

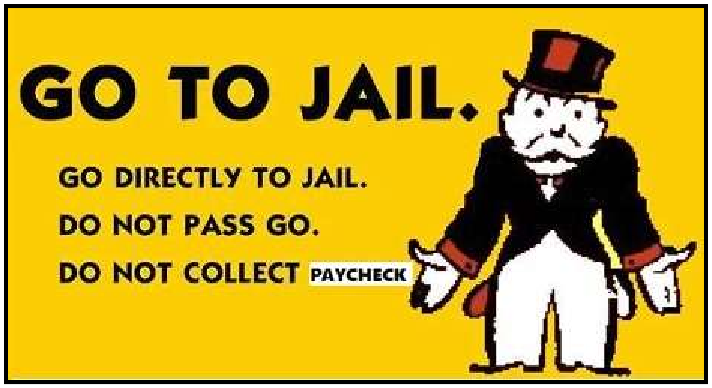
- Loss or compromise of classified or controlled sensitive information
- Weapons systems cloned, destroyed, or countered
- Loss of technological superiority
- Economic loss
- Physical harm or loss of life

Fighting the Insider Threat

DETER

DETER

To prevent an action by fear of consequences.



Take Annual Training!

Be Aware!

Read The Signs!

DETECT

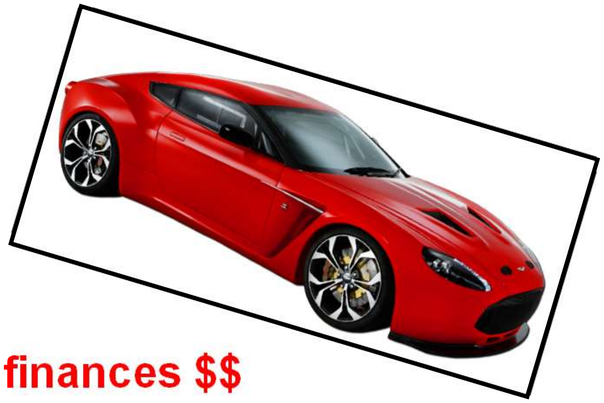
DETECT

To discover, identify, or investigate the presence or existence of something.

Detecting potentially malicious behaviors

Taking classified information

Change in attitude



Unexplained finances $$

MITIGATE

MITIGATE

To make less severe, serious, or painful.

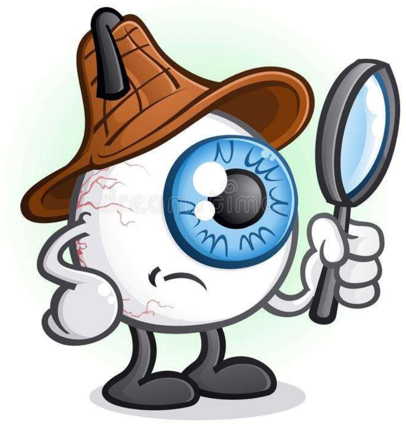
Self Report!

Good news: I've secured the office printer from hackers!
Anybody know why I can't print all of a sudden?
MIT IST

Take Annual Training!

Recognizing the Insider Threat

How to Recognize an Insider Threat



- Repeated security violations and a general disregard for security rules
- Failure to report overseas travel or contact with foreign nationals when required to do so
- Bringing an unauthorized electronic device into a controlled area
- Discussing classified info on a non-secure telephone or in non-secure emails or text messages
- Attempting to enter areas not granted access to or accessing information not needed for job
- Being disgruntled to the point of wanting to retaliate

Recognize the Insider Threat (continued)

Behavioral Indicators*
- Depression
- Stress in personal life
- Exploitable behavior traits:

– Use of alcohol or drugs

– Gambling

- Financial trouble
- Prior disciplinary issues

** These behaviors may also be indicative of potential workplace violence.*

Reporting the Insider Threat

Who to Report to?

Each employee has a responsibility to ensure the protection of classified and CUI entrusted to them. Be aware of potential issues and the actions of those around you and report suspicious behaviors to:

- Supervisors
- Security element
- Insider Threat Manager
- Law Enforcement
- Military Department CI Organization(e.g., NCIS)
- FBI

What to Report?

- Keeping classified materials in an unauthorized location (e.g., at home)
- Attempting to access classified information without authorization
- Questionable downloads
- Using an unclassified medium to transmit classified materials
- Discussing classified info on a non-secure telephone or in non-secure emails or text messages
- Removing the classification markings from documents
- Unnecessary copying of classified material
- Sudden reversal of financial situation or a sudden repayment of large debts or loans
- Being disgruntled to the point of wanting to retaliate
- Repeated or unrequired work outside of normal duty hours
- Bringing an unauthorized electronic device into a controlled area
- Making threats to the safety of people or property
- Expressing loyalty to another country
- Concealing reportable foreign travel or contacts

Note: The above list of behaviors is not inclusive, it only depicts a small set of examples. While not all of these behaviors are definitive indicators that the individual is an insider threat, these actions should be reported before it is too late.

Failure to Report

- Military: Punitive action under Article 92 (UCMJ)
- Civilians: Appropriate disciplinary action under policies governing civilian employees
- Contractors: DoD 5220.22-M, NISPOM

All: Could lead to dishonorable discharge, loss of employment, loss of access (clearance), fines or loss of wages, or imprisonment.

Insider Threat Cases

Reality Winner – NSA Translator pled guilty to leaking classified docs about Russian interference in the 2016 elections. Sentenced to 5 years 3 months in prison; released early in June 2021.

Bryan Martin – Navy sailor pled guilty to four counts of attempted espionage. Accepted over $11K from an undercover FBI agent. Received dishonorable discharge, forfeiture of all pay and sentenced to 34 years in prison.

Stewart Nozette – Gov't scientist pled guilty to attempted espionage for providing classified info to a person he believed to be an Israeli intelligence officer. Sentenced to 13 years in prison.

James Michael Wells – US Coast Guard civilian employee received life sentence for killing two coworkers.

Jin Hanjuan - Software engineer stopped by DHS at Chicago airport. Had more than 1,000 classified electronic and paper docs. Sentenced to four years in federal prison for stealing Motorola trade secrets and fined $20K; released on good behavior.

Insider Threat Cases

(continued)

Chelsea Manning (formerly Bradley Manning) – Responsible for unauthorized disclosure of classified info to WikiLeaks.

Nidal Hassan – Deadliest shooting on an American military base killing 13 people, injuring over 30 others.

Edward Snowden – Responsible for unauthorized disclosure of classified NSA surveillance programs.

Aaron Alexis – IT contractor responsible for killing 12 people at the Navy Yard.

John Beliveau – Former NCIS agent traded classified information in exchange for gifts and money.

Summary

IF YOU SEE SOMETHING

SAY SOMETHING

Questions

NAVSEA WARFARE CENTERS Carderock Division

Unauthorized Commitments (UACs)

NAVSEA WARFARE CENTERS Carderock Division

What is an UAC?

- An agreement made by a government representative who lacks the authority to obligate or commit appropriated funds on behalf of the Government, thus making the agreement non-binding (Federal Acquisition Regulation [FAR] 1.602-3).

- Any person lacking the proper authority who deliberately or unintentionally authorizes a supplier to provide goods or services to the Government creates an unauthorized commitment. The responsible individual may be held personally and financially liable for said commitment.

- A request for ratification must "establish whether the unauthorized commitment meets the ratification requirements set forth in." [FAR 1.602-3]

Summarizing the previous slide……

A UAC is an agreement that is not binding solely because the government representative who made it lacked the authority to enter into that agreement on behalf of the government

Personnel OTHER than Contracting Officers and Purchase Card Holders lack authority to bind the government!

A ratification request must establish whether the UCA meets the requirements for ratification as set forth in FAR 1.602-3.

Examples of UACs

A training class was scheduled and held BUT the cardholder had not paid for the class prior to personnel attending the first day of the class.

An unauthorized government employee requested locksmith services from a contractor knowing a contract was NOT in place and promised future payment.

A subject matter expert or Contracting Officer’s representative (COR) directed a contractor to perform out-of-scope work on a contract.

Examples of UACs *(cont.)*

A subject matter expert or Contracting Officer's Representative (COR) directed a contractor to perform additional tasking after the contractor had expended all the funding provided on the contract.

Personnel sent equipment to be inspected to the vendor before the vendor received authorization to perform the inspection via a contract or purchase card buy.   The equipment was sent with a shipping form clearly stating a $500 inspection fee. The contractor performed the inspection upon receipt of the equipment.

Scenarios

Scenario 1:

- **Question:** A Federal employee with purchase card authority of up to $3,500 enters into a contract with a hotel for a meeting space that costs $4,300.

- Answer: This is an UAC! => Reason: Total cost of the meeting space exceeds the cardholder's authority.

Scenarios *(cont.)*

Scenario 2:

- **Q: The program office has a contract for 20 working printers. One of the printers jams frequently and a new printer has been delivered as a replacement. The contractor is told to leave the old printer in place, because it still works.**
- **A: This is an UAC! => Reason: Contractor provided more than he/she is under contract to provide. Since the contract only permits 20 printers, the old printer should be removed when the replacement was delivered. The person interacting with the contractor should contact the *Contracting Officer* or *COR* and allow *them* to provide instructions to the contractor.**

Scenarios *(cont.)*

Scenario 3:

- **Q:** A supplier mistakes a request for information for an order and subsequently ships an item.

- A: This is NOT an UAC as long as: The person that received the item does NOT accept (or use) the delivered item. The person who receives the item should notify the Contracting Officer or COR and the vendor that mistakenly shipped the item.
- BEWARE: If a vendor emails a software update/license or subscription renewal to an employee BEFORE the vendor receives the contract, and the user downloads the update or renewal, this IS a UAC because the user downloaded the update, indicating it was accepted before it was authorized by a Contracting Officer/Purchase Card Holder.

UAC Statistics at Carderock

- FY 21: 3 ratified actions
- FY 20: 0 actions ratified

  2 actions resolved into a non-reportable status, with one paid by the unauthorized individual
- FY 19: 3 ratified actions

- FY 18: 1 ratified action

- FY 17:

  4 actions ratified
  - ➢ 5 actions resolved into a non-reportable status
  - ➢ 3 actions being paid by the unauthorized individual

Impacts of UACs

UACs must be ratified by a Contracting Officer, thus taking priority over other work that needs to be performed.

All UACs are reported to NAVSEA, and if NAVSEA has received more than seven (7), NAVSEA is required to report the UAC to Assistant to the Secretary of the Navy.

All UAC's over $50,000 and for repeat offenders must be approved at SEA00.

If NOT ratified, you are personally responsible to pay.

Even if ratified, you still may be subjected to disciplinary action.

Severe damage to government-contractor relationship

POC for UACs

If you need more information or have questions regarding unauthorized commitments, please contact our Policy Branch at:

Code02_Policy.fct@navy.mil.

Questions?

Wrap up